University of Plymouth

PEARL **https://pearl.plymouth.ac.uk**

04 University of Plymouth Research Theses 01 Research Theses Main Collection

2019

A Model for User-centric Information Security Risk Assessment and Response

Alohali, Manal

http://hdl.handle.net/10026.1/13698

http://dx.doi.org/10.24382/849
University of Plymouth

All content in PEARL is protected by copyright law. Author manuscripts are made available in accordance with publisher policies. Please cite only the published version using the details provided on the item record or document. In the absence of an open licence (e.g. Creative Commons), permissions for further reuse of content should be sought from the publisher or author.

Copyright Statement

This copy of the thesis has been supplied on condition that anyone who consults it is understood to recognise that its copyright rests with its author and that no quotation from the thesis and no information derived from it may be published without the author's prior consent.

Copyright © 2019 Manal Alohali

UNIVERSITY OF
PLYMOUTH

A MODEL FOR USER-CENTRIC INFORMATION SECURITY RISK ASSESSMENT AND RESPONSE

by

MANAL ABDULLAH ALOHALI

A thesis submitted to the University of Plymouth
in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Computing, Electronics and Mathematics

March 2019

Acknowledgements

Firstly, I give honor and praise to God Almighty for giving me strength and enabling me to complete my studies.

My special appreciation and sincere gratitude to my Director of Studies, Professor Nathan Clarke for his endless motivation, cooperation, support and professional guidance throughout this journey. This work would not have been possible without his immense knowledge and enthusiasm. I also wish to thank my second supervisor, Professor Steven Furnell for his time, insights and great efforts. I could not have imagined having a better supervisory team for my PhD study.

My heartfelt thanks to my family who incented me to strive towards my goal. Words cannot express how grateful I am to my husband and children for their understanding, patience and infinite encouragement. My special thanks to my sisters and brothers for their endless support and help.

In loving memory of my parents. May God bless them.

Finally, this research has been made possible by the scholarship granted to me by Princess Nourah bint Abdulrahman University, Saudi Arabia for which I am very thankful.

Author's Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Doctoral College Quality Sub-Committee.

Work submitted for this research degree at the University of Plymouth has not formed part of any other degree either at the University of Plymouth or at another establishment.

The following courses organised by University of Plymouth were attended: Unconscious bias, Diversity in the workplace, GDPR and information security, Health and safety, Introduction to EndNote, Immersive writing workshop, Overview to searching and accessing information resources, Matlab - An Introduction, Ms Project 2010 and Introduction to Qualitative research methods.

Publications:

1) Alohali, M., Clarke, N., Li, F. and Furnell, S. (2018). Identifying and Predicting the Factors Affecting End-users' Risk-taking Behavior. *Information and Computer Security*, Vol.26, Issue 3, pp.306-326.
DOI: 10.1108/ICS-03-2018-0037

2) Alohali, M., Clarke, N. and Furnell, S. (2018). The Design and Evaluation of a User-centric Information Security Risk Assessment and Response Framework. *International Journal of Advanced Computer Science and Applications,* , Vol.9, Issue 10, pp.148-163.
DOI: 10.14569/IJACSA.2018.091018

3) Alohali, M., Clarke, M., Furnell, S. and Albakri, S. (2017). Information Security Behavior: Recognizing the Influencers. *Computing Conference*, London, United Kingdom, 2017, pp. 844-853.
DOI: 10.1109/SAI.2017.8252194

4) Alohali, M., Clarke, N., Li, F. and Furnell, S. (2017). Identifying the Factors Affecting End-Users' Risk-Taking Behavior. *Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017)*, Adelaide, Australia, 2017, pp. 126-144.
DOI: 978-1-84102-428-8

Word count of main body of thesis: 68,624

Signed : ……

Date: ……

Abstract

A Model for User-centric Information Security Risk Assessment and Response

Manal Alohali

Managing and assessing information security risks in organizations is a well understood and accepted approach, with literature providing a vast array of proposed tools, methods and techniques. They are, however, tailored for organizations, with little literature supporting how these can be achieved more generally for end-users, i.e. users, who are solely responsible for their devices, data and for making their own security decisions. To protect against them, technical countermeasures alone has been found insufficient as it can be misused by users and become vulnerable to various threats. This research focuses on better understanding of human behavior which is vital for ensuring an efficient information security environment. Motivated by the fact that different users react differently to the same stimuli, identifying the reasons behind variations in security behavior and why certain users could be "*at risk*" more than others is a step towards developing techniques that can enhance user's behavior and protect them against security attacks.

A user survey was undertaken to explore users security behavior in several domains and to investigate the correlation between users characteristics and their risk taking behavior. Analysis of the results demonstrated that user's characteristics do play a significant role in affecting their security behavior risk levels. Based upon these findings, this study proposed a user-centric model that is intended to provide a comprehensive framework for assessing and communicating information security risks for users of the general public with the aim of monitoring, assessing and responding to user's behavior in a continuous, individualized and timely manner. The proposed approach is built upon two components: assessing risks and communicating them. Aside from the traditional risk assessment formula, three risk estimation models are proposed: a user-centric, system-based and an aggregated model to create an individualized risk profile. As part of its novelty, both user-centric and behavioral-related factors are considered in the assessment. This resulted in an individualized and timely risk assessment in granular form. Aside from the traditional risk communication approach of one message/one-size-fits-all, a gradual response mechanism is proposed to individually and persuasively respond to risk and educate the user of his risk-taking behavior.

Two experiments and a scenario-based simulation of users with varying user-centric factors has been implemented to simulate the proposed model, how it works and to evaluate its effectiveness and usefulness. The proposed approach worked in the way it was expected to. The analysis of the experiments results provided an indication that risk could be assessed differently for the same behavior based upon a number of user-centric and behavioral-related factors resulting in an individualized granular risk score/level. This granular risk assessment, away from high, medium and low, provided a more insightful evaluation of both risk and response. The analysis of results was also useful in demonstrating how risk is not the same for all users and how the proposed model is effective in adapting to differences between users offering a novel approach to assessing information security risks.

Table of Contents

List of Tables

List of Figures

Chapter 1 : Introduction and Overview

1.1 Introduction

With the rapid growth of technology and the wide range of 24/7 e-services provided by different devices such as laptops, smartphones, smart TVs, game consoles and wearable technology, the number of users is growing every day. The availability, and to some extent the ease of use of these technologies and services make it increasingly appealing to users who range from novices to technology-savvy users. Users can store, access and process all kinds of information such as business, personal, financial and medical data on a range of devices and infrastructure where each device has its own security requirements (Ledermuller and Clarke 2011; Allam et al. 2014). However, many risks are associated with these kinds of technologies/services such as privacy and information security risks. Users, who are solely responsible for their devices, data and for making their own security decisions, are arguably not well aware of such risks associated with the use of these devices (Mylonas et al. 2013; Jing et al. 2014).

The growth and popularity of the Internet has transformed our lives where Internet access is now considered as a necessity rather than a luxury. The number of Internet users increased from 2.94 billion users in 2014 to 3.8 billion users in 2017 where most homes have one or more devices connected to the Internet whether through wired or wireless communication through services offered by ISPs (InternetLiveStats 2017). Users spend time on the Internet performing many online activities such as online chatting, sending emails, browsing the web and socializing on social networks (Hasan and Hussin 2010; Kritzinger and Von Solms 2013). With this wide spread use of Internet, comes an increase in information security threats. This is evident as the number of created malware grew from 274 million in 2014 to almost 670 million in 2017 with a rate of 1.8 million threats introduced everyday (Symantec 2018) and an email malware rate of 1 in 131in 2016 compared to 1 in 244 and 1 in 220 in 2014 and 2015 respectively (Symantec 2017). During 2017, 29.4% of user computers around the world were subjected to at least one attack (Kaspersky 2017).

However, the presence of an uneducated or ill-informed user makes them an easy and attractive target for attackers. This is evident as employees mistakes are considered as one of the top threats to information security in organizations (Aloul 2010; Rao and Pati 2012; Hansch and Benenson 2014). With this continuously evolving threat landscape and the increased number of Internet users, the need for a security-aware user is expanded into a wider population to include everyone. This need is significant as they both pose and face risks. On the one hand, they pose risks as they are considered risk to others. On the other hand, they face risks as they are considered risk to themselves (Aloul 2010; Furnell and Clarke 2012; Kritzinger and Von Solms 2013).

Although they are solely responsible for the protection of their own devices and information, little evidence is found demonstrating that they are knowledgeable of information security threats and protection, and actually practicing it (Talib et al. 2010; Rao and Pati 2012; Kritzinger and Von Solms 2013). Indeed, it has been found that they are less willing to perform money-related and sensitive data tasks on some of these devices such as smartphones due to issues related to security, privacy, trust and usability (Zabaa et al. 2011; Mylonas et al. 2013). Furthermore, they have difficulties in using, understanding and reacting to security-related threats (Mensch and Wilkie 2011; Zabaa et al. 2011; Komatsu et al. 2013). Additionally, they have been found to feel they do not have the skills or knowledge to protect themselves, as a result, they often try to avoid security and depend on others to provide it for them. Users often view information security as complicated and not well understood which makes them rarely interested in learning about information security and how information security software works (Furnell et al. 2008; Wash and Rader 2011; Rao and Pati 2012). As security is considered a secondary task and not a primary task for users (Furnell and Clarke 2012; Harbach et al. 2014), educating them about information security threats is a challenging but a must to fight against these threats. Although this is a well-established and accepted approach in organizations where resources are, arguably, allocated to achieve the organizations' goals, it is a challenge in the case of users of the general public (Furnell and Clarke 2012).

Thus, considering the human aspects of security are vital for ensuring an efficient Information security environment that cannot depend on technology only. This implies the need to understand

users' perception of adopted Information security (Furnell et al. 2008; Wash and Rader 2011; Furnell and Clarke 2012; Metalidou et al. 2014). One cannot assume that users are always motivated to learn about Information security and practice it. Actually, there are situations of an aware user who knows how to protect himself but, simply, chooses not to, perhaps because they do not care, usability problems related to the used security control or simply because they do not consider themselves as targets (Albrechtsen 2007; Furnell and Clarke 2012; Shropshire et al. 2015). Further to that, the slow adoption of security controls is not only related to usability but also to the fact that users will only try to protect themselves from risks that are salient to them (Wash and Rader 2011; Harbach et al. 2014).

Maintaining information security generally focuses on the protection of Confidentiality, Integrity and Availability (CIA) of information. Therefore, an information security attack is affecting the CIA of assets (Kaur and Mustafa 2013). Managing and assessing information security risks in organizations is a well understood and an accepted approach used widely by enterprise organizations to provide a safe environment to carry out their business using the most cost-efficient and effective means (Tiganoaia 2012; ENISA 2014).

As risk is a common problem in many fields, many information security risk management methodologies were issued by national and international organizations such as The National Institute of Standards and Technologies (NIST) Special Publication 800-series (NIST 2012) and The International Standards Organization ISO/IEC 27000 (ISO 2011) or issued by professional organizations such as CORAS(CORAS 2014), Magerit (Magerit 2006), Mehari (Mehari 2007), OCTAVE (OCTAVE 2014) and CRAMM (Yazar 2011) or as research projects (Karabacak and Sogukpinar 2005). Unfortunately, these tools and methodologies are designed for organizations and not members of the public. Traditional Risk Assessment (RA) methods either treat devices as a business information system asset or as a single entity where vulnerability and threat assessment is made on the asset as a whole rather than the services that are used within the device (Komatsu et al. 2013). By focusing on the user not the device, increased security awareness through understanding and effectively communicating risk would arguably improve security behavior and lead to reduced security risks (Jing et al. 2014).

Further to that, although a number of risk assessment methodologies have contributed significantly to current knowledge and aimed at assessing risks for the general public, they are either too difficult to be used or understood by users or they could be used as an awareness tool with no guidance offered to users to make informed decisions. Moreover, most RA methodologies are static, i.e. time is not included explicitly in calculating risk. They are found to be ambiguous, imprecise and cannot effectively communicate the system's dynamic behavior, adversaries and actors to system stakeholders. Threats and vulnerabilities that vary overtime are identified using horizontal data with static time frame (Sadiq 2010). Additionally, they are platform dependent. Thus, there is a need for a platform independent and dynamic information security RA model that continuously assess and adaptively communicate risks in timely manner on both system and user behavior level. This implies that a structured approach tailored for users of the general public is needed to help them assess, analyze and make an informed decision regarding the risks they are exposed to.

1.2 Research aims and objectives

The research builds upon existing research on Information Security Risk Management and Communication in which the issues of awareness and risk communication will be considered. It will seek to develop a comprehensive and continuous User-Centric Risk Assessment and Response model. Further research will be made to understand how users from the general public make risk informed decisions and the relation between different users' characteristics, i.e. user-centric factors and their security behavior. A novel approach to individually and adaptively assess and communicate risks will be developed that focuses specifically on factors such as user behavior, awareness, and timeliness. Key to this work will also be the development of a number of risk estimation models from which this framework will operate. The effectiveness and reliability of the proposed models will also be evaluated.

In order to achieve this, the research objectives are established as follows:

1. To develop a current state of the art understanding of Information Security Risk Assessment methods.

2. To investigate the current approaches in security awareness, usability and human aspects of information security.
3. To identify the factors that influence user's risk taking behavior.
4. To explore the extent in which users are making risk informed decisions.
5. To analyze the relationship between differences in users' characteristics (user-centric factors) and their risk-taking behavior.
6. To propose a novel model for User-centric Risk Assessment and Response that assesses risks on both user and system level and generate an individualized risk profile accordingly.
7. To develop a novel approach in security awareness and usability to communicate risks effectively to users by designing a communication that efficiently and individually interacts with users.
8. To propose novel risk models that adapt to user's-centric factors when calculating risk of both system and user level risks and generate an aggregated risk score/level.
9. To design a scenario based simulation from which the models will operate. In this scenario based simulation, various users with different combinations of user-centric factors are involved to evaluate the effectiveness, reliability and feasibility of the proposed model.

1.3 Thesis Overview

To address the aforementioned objectives, this thesis is organized into eight chapters. The research problem, aims and objectives are introduced in Chapter 1.

The **second** chapter presents a literature review of Information Security Risk Management (ISRM) methodologies. It provides an overview of the ISRM process with a focus on Information Security Risk Assessment (ISRA). To develop a better understanding, it discusses and analyzes various ISRA approaches and methodologies whether those tailored for organizations or those intended for users of the general public. Not limited to that, enhancements to such methodologies are presented discussing both their advantages and disadvantages. This gives an overview of some of the current issues and challenges related to ISRA.

The **third** chapter investigates the current approaches in security awareness, usability and human aspects of information security using a systematic literature review. It discusses security awareness, training and education, gives a closer look at the current end-users', i.e. users, classifications and suggests another one. Additionally, current methods used to raise security awareness of users from the general public are presented. Risk communication, learning styles and delivery methods are also discussed. From this review, several key behavioral influencers are identified to be essential when educating and directing user's security behavior. This chapter concludes by outlining that risk is not the same for all users and that a number of factors play a role in shaping his risk-taking behavior.

Unlike other surveys that are limited in their scope, the **fourth** chapter presents a user survey study that explores user's security behavior from a holistic perspective including security behaviors from multiple domains such as data management and authentication. The study goes further to investigate the relationship between various user-centric factors and user's risk-taking behavior. A more complete set of analysis provides a more applicable understanding of what significant relations exist. Therefore, being identified the reasons behind variations in user's security behavior and why certain users are at-risk more than others is a step towards protecting and defending users against security attacks.

Capitalizing on the previous findings, the **fifth** chapter proposes a novel User-centric Risk Assessment and Response (UCRAR) model that goes beyond the traditional one-size-fits-all approach. The model intends to provide a comprehensive framework for individually and continuously assessing and communicating information security risks in a timely manner. The novelty of the proposed model depends upon four significant aspects: the continuous monitoring of user's behaviors, an aggregated risk score/level based upon risk assessment on both the user and system level, an individualized risk profile and a gradual, persuasive and individualized response mechanism. These aspects are utilized to enhance user's risk taking behavior and transform him from being ill-informed to a security minded user who is able to make a risk informed decision. This chapter provides detailed explanation of the proposed model with regards to its components, processes and its operational flow.

As UCRAR provides a mechanism for understanding both system and user/behavior risk and how to respond to them, the **sixth** chapter presents a novel proposed mechanism for estimating/calculating such risks. As part of the novelty of the proposed approach and aside from the traditional risk calculation formula, three risk estimation models are proposed: a user-centric, a system-based and an aggregated risk estimation model. These models are utilized within the functionality of the Risk Assessment component of UCRAR. The novelty of these models depend upon a suggested categorization of behaviors and the consideration of significant correlations between user-centric factors and user's behavior among other factors when estimating risk.

The **seventh** chapter discusses and analyzes the evaluation process of the proposed model through the design and implementation of a scenario based simulation from which the models will operate. This involved various users with different combinations of user-centric factors to evaluate the effectiveness, reliability and feasibility of the proposed approach. According to the proposed model, risks were assessed and results analyzed for each user/behavior. The analysis of simulation results is useful in demonstrating how risk is not the same for all users and how the proposed model is effective in adapting to differences between users. Furthermore, it provides an indication that risk could be assessed differently for the same behavior based upon a number of user-centric and behavioral related factors resulting in an individualized and more realistic risk score/level.

The **final** chapter presents the main conclusions derived from this research. It also highlights the achievements, limitations and opportunities for future work.

A Thesis flowchart is as in Figure 1.1

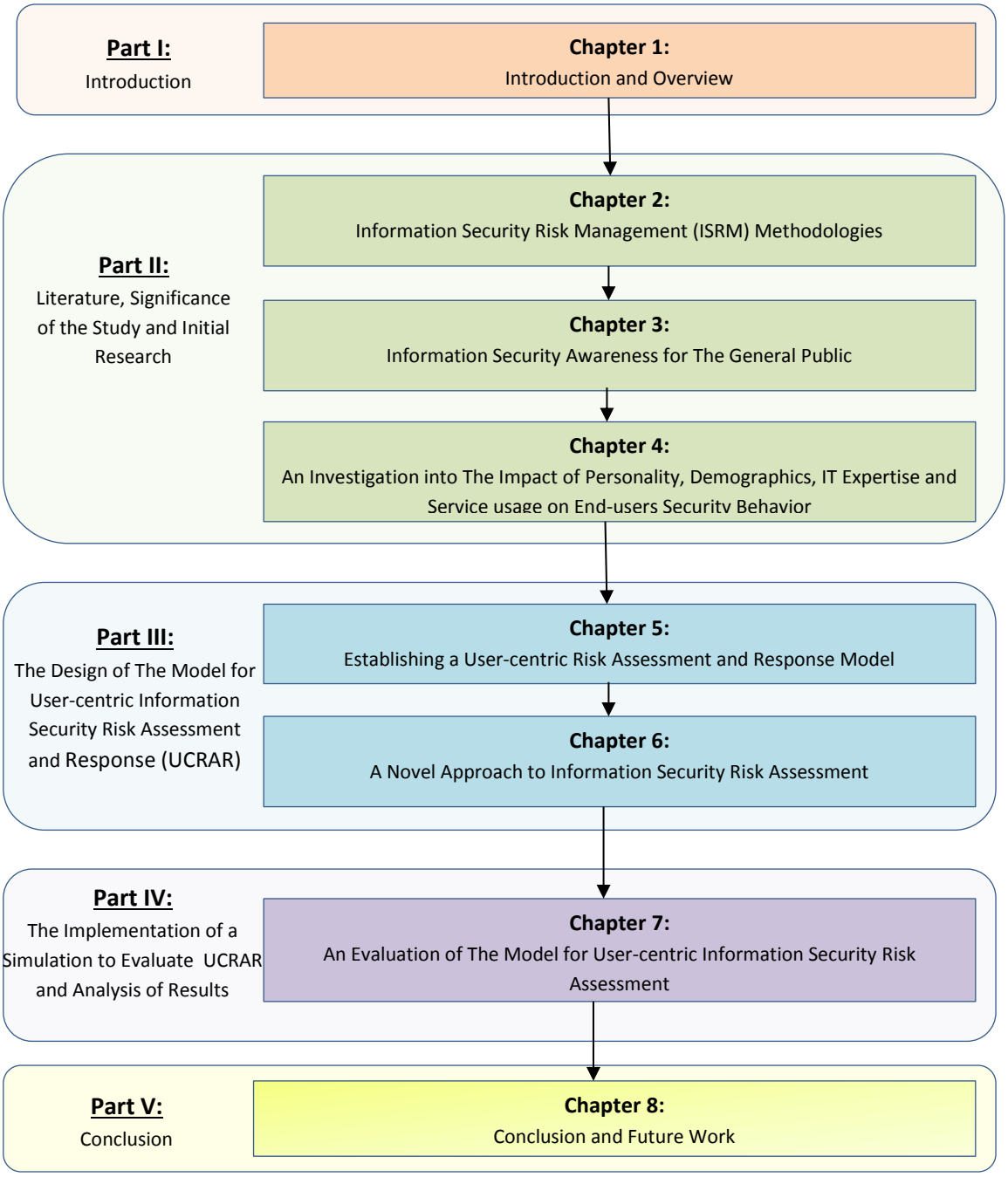

Figure 1.1: Thesis Flowchart

Chapter 2 : Information Security Risk Management (ISRM) Methodologies

2.1 Introduction

Information security is to provide confidentiality, integrity and availability of information through the protection of information and information systems from unauthorized access, disclosure, use, modification, disruption, modification or destruction (NIST 2012). The security threat landscape is complex and rapidly evolving as almost 2 million pieces of threats are introduced daily (Symantec 2018). Organizations, for example, major security concerns are about the confidentiality, integrity and availability of their IT systems. The risk of sensitive information leakage and modification, for example, through social networking, cloud computing or Bring Your Own Device (BYOD) technologies may result in significant damage to organization's revenue, reputation and competitive advantage (Bojanc 2013; Webb et al. 2014). Actually, this is not limited to organizations and include users from the general public.

Traditionally, information security was a technical discipline to provide the maximum security level in which threats were prevented by a technical solution only (Bojanc 2013). It was later realized that information security is a problem that cannot be resolved by technology only, but there are other aspects to it such as processes and economics (AlAwawdeh and Tubaishat 2014). Moreover, users are frequently identified as the weakest link in information security. The high rate of advancement in technology and the increasing number of developed and updated Information Technology (IT) systems for various sensitive and critical applications such as e-Government, e-Health and e-Banking forces a challenge in managing and assessing the risks faced by these systems especially information security risks (Sulaman et al. 2013; Webb et al. 2014). Indeed, this assessment is highly required as a step towards mitigating these risks. Managing and assessing information security risks is a well understood and accepted approach. It is usually expensive, time consuming and done by experts and professional risk assessors (Bojanc and Blazic 2013).

This chapter begins with an explanation of the ISRM process in section 2. The current RA methodologies are reviewed in section 3 and enhancements to these methodologies are discussed in the following section. ISRA for the general public is reviewed in section 5 followed by a discussion in section 6. Finally, a conclusion is presented.

2. 2 The ISRM Process

To better describe the process of ISRM, two definitions are given by two international standardized organizations, ISO and NIST. As defined by The International Standards Organization (ISO 2011), Risk Management (RM) is the coordinated activities to control and direct the organization with respect to risk. The activities of ISRM are as shown in Figure 2.1.

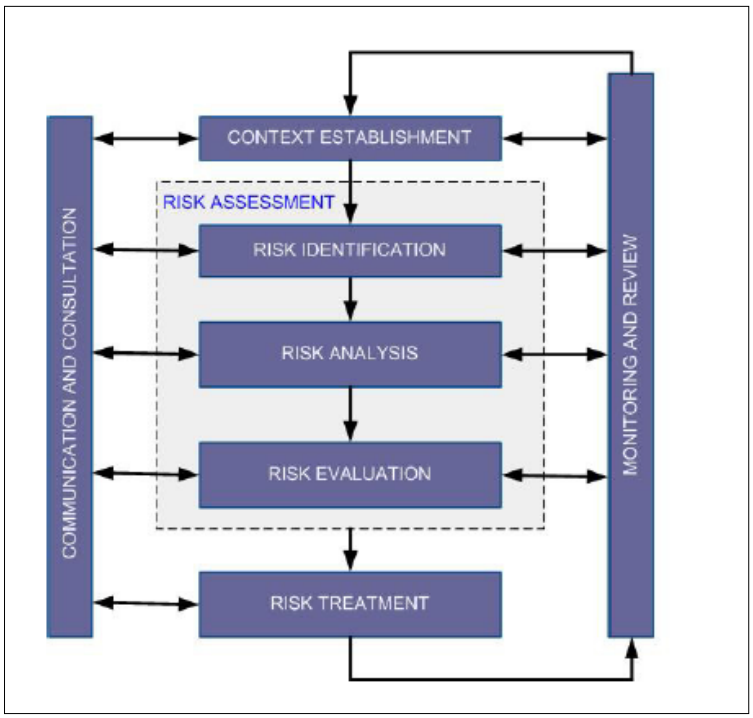

Figure 2.1: The Risk Management Process (ISO 2011)

This definition is close to that of The National Institute of Standards and Technologies (NIST 2012) who defines ISRM as the program and supporting processes to manage information security risks to organizational operations, individuals, assets, other organizations and the Nation. It includes the following activities:

1- Establishing the context of risk-related activities.

2- Risk Assessment

3- Responding to risk

4- Risk monitoring over time.

Thus, the classification of ISRM activities is not final and maybe used to describe a process that includes some of the other activities (Sulaman et al. 2013). Regardless of how ISRM activities are classified, the main goal is for organizations to determine if they are safeguarding their information assets by using the most cost effective and efficient means. An organization has to determine the needed and accepted level of security, where this level is determined by RM (Shedden et al. 2011; Bojanc and Blazic 2013; Webb et al. 2014). Therefore, ISRM establishes the basic security elements that are assets and their owners, vulnerabilities, threats, risks and measures (Bojanc and Blazic 2013).

In principle, risk is defined as the effect of uncertainty on objectives (ISO 2011). In the context of information security, risk is associated with the potential that a vulnerability(ies) of an information asset or group of information assets being exploited by a threat(s) thereby causing harm to an organization (ISO 2011). This implies that risks can only exist with the existence of an exploitable vulnerability. A further definition is given by NIST (NIST 2012) who defines risk as the measure of the extent to which an entity is threatened by a potential circumstance or event, and as a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence. In this static risk model, time is not incorporated as a variable, so no description is included to describe consequences. However, a more dynamic risk model is required that considers time. This will result in different types of actions taken based on the different phases of risk scenario. As the consideration of security risks is an important component of RM, many factors relate to information security risks whether managerial, human and/or technical (Van Cleef 2010). Moreover, risk components that should be considered during the process of risk identification are threats, vulnerabilities, assets, impacts and likelihood.

In the literature, threats tend to be used to refer to the potential cause of undesired incidents that may cause damage to the system or organization. It can range from natural disasters to innocent and simple employees mistakes (ISO 2011; NIST 2012; Bergomi et al. 2013; Bojanc and Blazic 2013).

Whilst assets, whether tangible or intangible, are defined as anything of value to an organization, threats have either direct or indirect impacts on assets (Yazar 2011). Furthermore, threats impacts on information assets include the destruction, modification, theft, disclosure and/or the denial of service i.e. service interruption (NIST 2012; Sulaman et al. 2013). However, threats could be categorized as physical damage, natural events, loss of essential services and technical failures (ISO 2011). Whereas a vulnerability, is the weakness in an information asset that can be exploited by a threat, the likelihood or probability is the chance that a threat can exploit a vulnerability or a set of vulnerabilities (ISO 2011; NIST 2012). Although the vulnerability in software is the major cause of security incidents, it is found that many incidents were related to humans such as the use of weak passwords, misunderstanding of security policies and visits to suspicious websites (Van Cleef 2010; Bojanc and Blazic 2013; Sulaman et al. 2013; AlAwawdeh and Tubaishat 2014).

After establishing the context, the process of ISRM starts by identifying and determining a list of possible risks, these risks are analyzed by combining the expected impact and the probability of each risk. Based on risk analysis results, risks are prioritized. Finally, the identified risks are mitigated or treated by reducing their consequences or probability of occurrence through the selection and implementation of appropriate controls and measures or by transferring these risks to another organization by outsourcing or insurance company. Another way of treating the identified risks is by avoiding or eliminating the risk's source or asset's exposure to it, i.e. risk avoidance. This is done when the severity of the risk impact outweighs the benefits of using or having a particular asset such as open connectivity to the Internet. However, if the cost of insuring or investment against the risks are greater over time than the sustained losses or asset value, then an organization may simply choose to accept the risk as part of its business operations (Yazar 2011; Bojanc and Blazic 2013; Sulaman et al. 2013; Webb et al. 2014).

2.2.1 Risk Assessment (RA)

RA has been discussed in the literature as a critical step in the risk management cycle. The International Organization for Standardization (ISO 2011) defines RA as the overall process of risk identification, analysis and evaluation. In this process, information assets are identified and risks to

these assets are identified and evaluated. Threats, vulnerabilities and harmful incidents that may affect information's confidentiality, integrity and availability are systematically identified by performing a methodical analysis of organization's assets. The National Institute of standards and Technology (NIST 2012) states that RA is synonymous to risk analysis where it incorporates threat and vulnerability analysis and considers the planned or in place security controls to mitigate the risks. It is worth noting that RA is a discrete non-continuous activity. Thus, it is initiated either when needed or at regular time intervals. However, a prior step to RA is risk identification. Various techniques could be used to improve risk identification's accuracy and completeness such as Delphi methodology and brainstorming (ISO 2009).

There are various information security standards by organizations such as ISO/IEC 27005:2011(ISO 2011) and NIST SP 800-30 (NIST 2012). Additionally, various RA methodologies were developed by professional organizations to meet specific requirements and therefore incorporate different steps, objectives, level of application and structure. Examples of such methodologies are CRAMM (Yazar 2011), CORAS (CORAS 2014), OCTAVE (OCTAVE 2014), Magerit (Magertit 2006) and Mehari (Mehari 2007) that have been fully or partially adopted by organizations to identify, analyze and treat their information security risks.

These methods are either quantitative, qualitative or semi-quantitative in nature. In quantitative methods, the identified risks probability and consequences are expressed numerically. Even when risk is quantified in scalar values, there is no exact risk value because of the uncertainty and subjectivity in defining likelihood and severity of consequences (Bhattacharjee et al. 2012). While in qualitative methods, the probability and consequences of identified risks are expressed through a qualitative subjective rating scheme using varying scales such as "high", "medium" and "low". However, a combination of qualitative and quantitative methods, semi-quantitative, could be used. To reveal major risks and to get a general indication of the risk level, a qualitative estimation could be used first. Then a quantitative analysis could be used later. Consequences and probability are specified using numerical rating scales and used in a formula to produce risk level (Samy et al. 2010; Ledermuller and Clarke 2011; Yazaar 2011; Sulaman et al. 2013).

Although qualitative methods are subjective, they are descriptive and easier to understand by all related personnel. They could be used to identify risks that need further analysis (ISO 2011). However, these methods are subjective since they rely on expert's security background, not efficient since two risks that are classified at the same ranking scale level are difficult to compare and are expensive since they require human expertise. Furthermore, a major disadvantage of qualitative methods is that the results achieved are general and during the process of appropriate security measures selection, cost benefit analysis is more difficult (Bergomi et al. 2013; Bhattacharjee et al. 2013).

On the other hand, quantitative methods give a more accurate risk image and could be linked directly to the organization's information security objectives and concerns. They allow more accurate risk events analysis where parameters are used in the RA process can be designed in many theoretical and mathematical models where results are in number forms which can be easily compared. Since it relies on historical data, then the lack of such data on new vulnerabilities and threats may affect the accuracy of such an assessment (Saleh and Alfantookh 2011; NIST 2012; Paintsil 2012).

Samy et al. (2010) and Webb et al. (2014) argue that most of existing RA methods rely mainly on rough estimations or guesswork of skilled risk assessors to estimate the probability and consequences associated with each risk. This is due to the lack of availability of security incidents data due to several reasons such as financial constraints, unreported cases or the inability to identify emerging indications of threat types that change over time. This results in wrong decisions with regards to the appropriate information security measures taken and to the time and effort wasted in controlling the wrong things (Shedden et al. 2011).

Given that almost 90% of reported security incidents resulted from exploits against software vulnerabilities whereas human-error was considered as one of the top threats to information security and almost two million pieces of malware introduced every day (Aloul 2010; Wu and Wang 2011; Rao and Pati 2012; Hansch and Benenson 2014; Symantec 2018) the need for a usable security tool that calculates and assesses risk on both system and user level in a timely manner is essential to

protecting users from threats and vulnerabilities and, thus, reducing the overall information security risks.

Information Security Management System (ISMS) represents framework design as an area of information security research to calculate information system's risks using various security techniques. Among those techniques is Vulnerability Management that is represented by The Security Content Automation Protocol SCAP (Waltermire et al. 2011; Takahashi et al. 2013). To communicate security information, SCAP provides several standard specifications, including Open Vulnerability and Assessment Language (OVAL) (oval.mitre.org) which is " *an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services"* (Oval.mitre.org) ,Common Vulnerabilities and Exposure (CVE) which is " *a dictionary of common names (i.e., CVE Identifiers) for publicly known cybersecurity vulnerabilities*" (cve.mitre.org) and Common Platform Enumeration (CPE) which is " *A structured naming scheme for information technology systems, software and packages*" (nvd.nist.gov/cpe.cfm).

The Common Vulnerability Scoring System (CVSS) is a scoring system that provides a standard specification that measures the severity of software vulnerabilities (Mell et al. 2007) and a widely used cybersecurity model (Wu and Wang 2011; Spanos et al. 2013; Takahashi et al. 2013; Wright et al. 2013; Allodi and Massacci 2014; Alsaleh and Alshaer 2014; Holm and Afridi 2015). In this scoring system, currently in its third version, three metrics are used to quantify the severity of vulnerabilities as follows:

1. ***Base metrics***: They measure the fundamental and intrinsic vulnerabilities characteristics that do not change over time or different environments.
2. ***Temporal metrics***: They measure vulnerabilities attributes that do not change among environments but over time.
3. ***Environmental metrics***: They measure vulnerabilities characteristics that are unique and relevant to a particular environment.

The National Vulnerability Database (NVD) is "*The U.S Government repository of standards based vulnerability management data using SCAP*". It is a valuable source of security knowledge and publically available online (nvd.nist.gov). Each NVD record contains CVE-id, vulnerable software list, vulnerability published date and time , CVSS base metrics and scores and so on. NVD uses CVSS to measure vulnerabilities severity which provides evidence of the wide and accepted adoption of CVSS by the security community (Spanos et al. 2013). Moreover, it is often used as a metric for risk (Allodi and Massacci 2014).

As Base and Temporal scores are scored by security professionals, system users such as system administrators are the ones to provide Environmental scores. However, this is rarely done in practice especially that Temporal scores do not have search fields in NVD. Consequently, the Base score, from the point of view of many users, is actually considered as the CVSS (Holm and Afridi 2015). NVD offers a publically available online calculator to calculate the CVSS score in both Version 2 and Version 3. Vulnerabilities severity is measured on a 0-10 scale of three severity states, High, Medium and Low. As a matter of fact, this metric is an aggregation of two other metrics, Exploitability and Impact (Mell et al. 2007; Alsaleh and Alshaer 2014). Although many researchers examined the accuracy and validity of the CVSS scoring algorithm (Liu and Zahng 2011; Holm et al. 2012; Allodi and Massacci 2012; Allodi et al. 2013), it is suggested not to use it as a sole risk factor to determine the security risk level and that additional risk factors to be used.

2.3 RA Methodologies

There are a number of different ISRM methodologies and guidelines around the world that differ in their approach, level of detail, usage complexity and applicability to different-sized organizations (Paul and Davillier 2014). Among them are as follows:

1. International organizations:

    1.a. NIST SP 800-30

    1.b. ISO/IEC 27005:2011

2. Professional organizations:

    2.a. CRAMM

    2.b. OCTAVE

    2.c. CORAS

3. Research project:

    3.a. ISRAM

These methodologies are selected based on ENISA (2014) that consists of seventeen methods. Of these methods, four are as far the most commonly used, i.e. have acceptance in the market, with geographical spread and are well documented, i.e. provide publically available information. The remaining methodologies may be considered as extensions or derivatives of the other selected methodologies. However, since the list by (ENISA 2014) is none-exhaustive and is an open list, two methodologies were added. First, CORAS is added to this list as an example of a model-based RA methodology, i.e. the system is conceptually modeled before risk is estimated and evaluated, whilst the remaining methods are list-based, i.e. risk findings are documented in structured lists and risk is estimated based on best practices, standards or checklists. On one hand, structured lists are easier to create but require a lot of time to communicate security risk findings. On the other hand, model-based approaches facilitate early risk elements discovery because no information is hidden among irrelevant details (Paintsil 2012). Second, ISRAM is added to this list as an example of a research project with a quantitative RA methodology from Turkey. Furthermore, these methodologies have different analysis approaches towards risk. As stated by (NIST 2012), these approaches could be divided into:

- Threat-oriented where the method starts with the identification of threat sources and events.
- Asset/Impact oriented where the method starts with the identification of high-level assets or impacts.
- Vulnerability-oriented where the method starts with the identification of a set of predisposing conditions or vulnerabilities.

Although the same risk factors are considered in all methods resulting in the same RA activities, difference in RA starting point may cause some bias in the RA result. This is because some risks not

being identified. Therefore, the analysis effectiveness can be improved by complementing one analysis approach with another (NIST 2012; Paintsil 2012; Sulaman et al. 2013).

The classification approach of ISRM methodologies is shown in Figure 2.2. The reviewed methodologies are classified according to origin, assessment approach, analysis approach, the way the targeted system is documented and tool support.

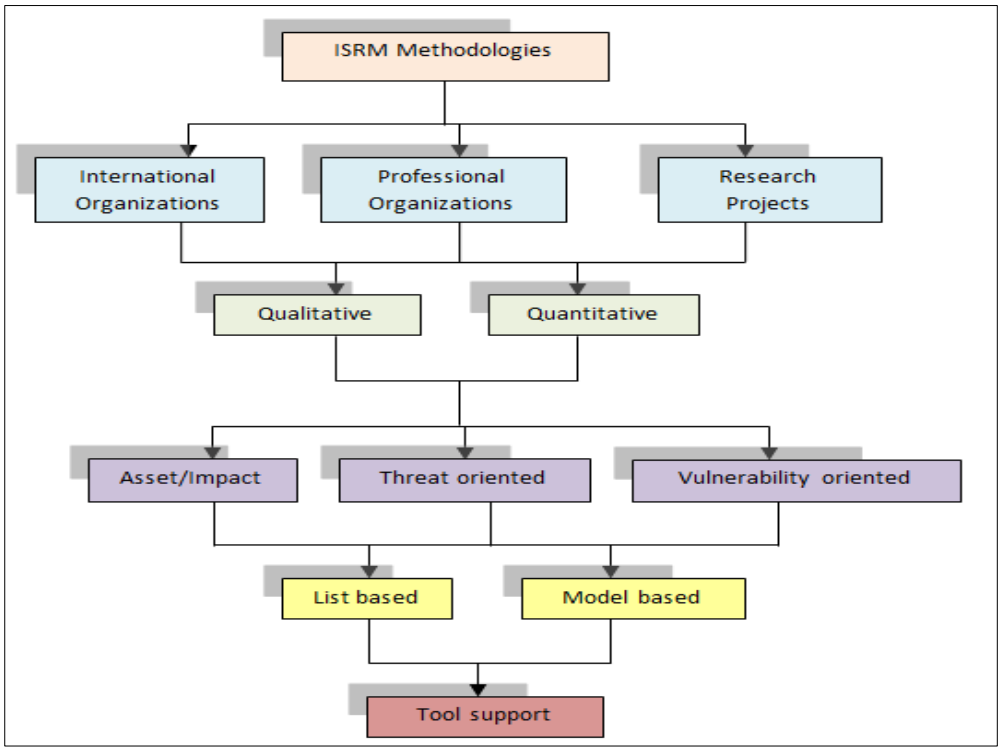

Figure 2.2: Classification approach of ISRM methodologies

2.3.1 NIST SP 800-30

The National Institute of Standard and Technology of the US Department of Commerce issued a special publication of the report NIST SP 800-3- in 2012. This report provides detailed identification and guidance of the issues to be considered when implementing ISRM and ISRA which are mainly based on US regularity issues (NIST 2012).

RA is used to " Identify, estimate and prioritize risk to organizational operations, assets, individuals, other organizations and the Nation resulting from the operation and use of information systems". It is conducted at Tier1 organizational level, Tier2 mission/business process level and Tier3 information system level of the risk management hierarchy. At Tiers 1 and 2, RA is used to evaluate

information security risks related to management activities, organizational governance and information security programs funding. At Tier3, RA is used to support risk management framework implementation of security categorization, selection of security controls, implementation, assessment, authorization of controls and monitoring. RA process is carried out in four basic steps as shown in Figure 2.3.

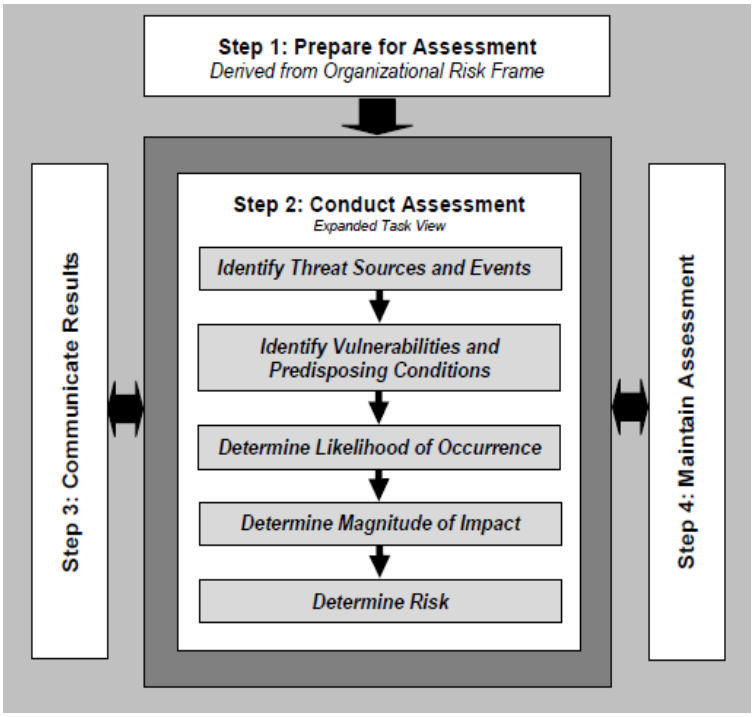

Figure 2.3: NIST Risk Assessment Process (NIST 2012)

Step 1: Preparing for the Assessment

The objective of this step is to establish the RA context by identifying the assessment purpose, scope, threats, vulnerability and impact that will be used in the process of RA. Moreover, the risk model, assessment approach whether quantitative, qualitative or semi-quantitative and the analysis approach whether threat-oriented, asset/impact-oriented or vulnerability-oriented are also identified.

Step 2: Conducting the Risk Assessment

The objective of this step is to produce an information security list of prioritized risks that could be used to make risk response decisions (Rajabhandari 2013). This is achieved by identifying vulnerabilities, threat sources, potential threat events and their likelihood and impact.

Step 3: The Communication and Sharing of RA information

The objective of this step is to ensure that appropriate risk related information is made available to decision makers from across the organization to guide and inform risk decisions.

Step 4: Maintaining the Risk Assessment

The objective of this step is to support the ongoing review of risk management decisions and the monitoring of the identified risk factors on an ongoing basis and understand changes to them.

NIST SP 800-30 has a qualitative approach to RA where it depends on narrative risk descriptions. The main goal is to help organizations in managing risks by providing a basis to develop an effective program for risk management. Furthermore, definitions and the necessary guidance to assess and mitigate risks are provided. Moreover, it provides requirements and general rules for system characterization but no specific model is provided to characterize assets and interrelation between them. It provides a high-level view of RM with a one-size-fits-all methodology. Thus, there is a lack of recommendations and guidelines on how it could be tailored for small, medium and large organizations. Therefore, there is no reference to other risk management techniques and methods. However, NIST SP 800-30 is publically available and has been reviewed by industry professionals and Government (NIST 2012).

2.3.2 ISO/IEC 27005:2011

This is a conceptual international standard issued by the International Standards Organization (ISO) to provide ISRM guidelines in an organization. However, this standard does not offer a specific ISRM methodology where an organization has to adopt any of the existing methodologies depending, for example, on the industry sector or risk management context (ISO 2011). Risk management process is as shown in Figure 2.1.

The activities of RA and Risk Treatment (RT) could be iterative resulting in increasing the assessment details and depth at each iteration. This provides balance between time and effort in identifying controls while high risks are still appropriately assessed. The first iteration is a high level RA, where the business values of information assets and the organization's business point of view of

risks are considered. This is followed by in-depth processes of assets identification and valuation and threat and vulnerability assessment (Bhattacharjee et al. 2012). RA is carried out in the following steps:

Step 1: Risk Identification

The objective of this step is to identify what could happen to cause a potential loss and how, where and why this loss might happen. In this step, assets, threats and their sources, existing controls, vulnerabilities and impacts on assets are identified.

Step 2: Risk Analysis

The used RA methodology maybe quantitative, qualitative or semi quantitative. In this step, the consequences and incident likelihood are assessed in order to determine the level of each identified risk.

Step 3: Risk Evaluation

The objective of this step is to prioritize each of the identified risks according to the risk evaluation criteria. As a result, decisions about future actions are made such as whether to undertake an activity or not. The used criteria should consider organizational objectives, stakeholder views and be consistent with the defined ISRM context.

ISO/IEC 27005:2011 is a standard approach towards RA. Thus, it gives an outline of a systematic and structured approach towards RA taking into account the organizational aspects of processes, people and technology. It merely gives recommendations on the scope and applicability of either a quantitative or a qualitative approach to RA. However, the process of RA is described at an abstract level where a third-party method for RA is needed to carry out a more comprehensive RA. Thus, it is flexible in choosing such method where some advice is given on how to choose and use such a method.

2.3.3 CRAMM

The CCTA Risk Analysis and Management Method (CRAMM) was issued by the Central Computer and Telecommunication Agency in 1985 by the United Kingdom Government. It has gone under major revisions and currently in version 5.00. This RA and management method utilizes both

quantitative and qualitative measures. CRAMM provides guidance for compliance with the British Standard for Information Security BS7799 (Yazaar 2011). It is supported by a tool with the same name that comes in three versions, CRAMM Expert, CRAMM Express and BS7799 Review (Tiganoaia 2012). CRAMM is divided into three main steps that relate to technical and non-technical aspects of security. Each step is supposed to answer a specific question.

Step 1: Identification and Valuation of Assets:

This step is concerned with answering the question of "Is there a need for security?". For data collection, interviews, meetings and structured questionnaires are used to set security objectives, boundaries, scope of study and to identify and estimate the value of assets. Data assets values are derived from the impacts of Confidentiality, Integrity and Availability (CIA) on them by describing the worst-case scenarios and the possible consequences of data not being available, destroyed, disclosed or modified. Physical assets and application software are valued by interviewing the "support personnel" in terms of their reconstruction or replacement cost. All these values are quantified on a scale of 1-10.

Step 2: Threat and Vulnerability Assessment:

This step is concerned with answering the question of "What and Where is Security Needed?". Threats and vulnerabilities are identified by asking questions to related stakeholders. CRAMM quantifies threat/asset levels on a five point scale from "very low" to "very high" and vulnerability/threat levels on a scale of "low, medium, high". Finally, for each asset group, risk is calculated by using a predefined value risk matrix to compare threat and vulnerability levels to asset values.

Step 3: Selection of Countermeasures and recommendations:

This step is concerned with answering the question of " How can security needs be met?". Based on the findings of step2, a set of applicable countermeasures are produced to manage the identified risks. They are compared against existing (if any) countermeasures in order to identify weakness or over-protected areas.

CRAMM is best for large organizations such as Governmental Departments (Feng et al. 2014). It is a qualitative RA methodology that has an asset-centric Risk analysis approach with no steps for implementation of security controls or follow up. The process of RA is mostly automated where CRAMM has an extensive free tool support and a database of more than 300 security controls and certification tools. Thus, it can only be used with this dedicated tool. However, the assessment process using CRAMM could be complex and lengthy where expert knowledge is needed. Regardless of its complexity, the assessment could be set according to needs.

2.3.4 OCTAVE

"Operationally, Critical, Threat, Asset and Vulnerability Evaluation" OCTAVE is a process-driven methodology developed by the Carnegie Mellon University Software Engineering Institute (SEI), USA to assess the information security needs of an organization. One major advantage of OCTAVE is its ability to link its organizational objectives and goals to information security goals and objectives (Panda 2009). It focuses on security practices, strategic issues and organizational evaluation rather than system evaluation, tactical issues and technology. Threats are categorized as human using network access, human using physical access, system problems and problems that cannot be controlled by organization such as earthquakes and floods (Rajabhandari 2013). SEI developed three OCTAVE methodologies (OCATVE 2014):

2.3.4.1 OCTAVE Method

This method is designed for large multi layered hierarchy organizations to maintain their own computational infrastructure in 1999. It uses a three-phase approach, organizational view, technological view and risk analysis, with eight processes to create a comprehensive view of the organizations security needs by examining both organizational and technological issues. As a result, a security protection strategy and plan to address the identified risks is produced. The phases and processes of OCTAVE are as shown in Figure 2.4.

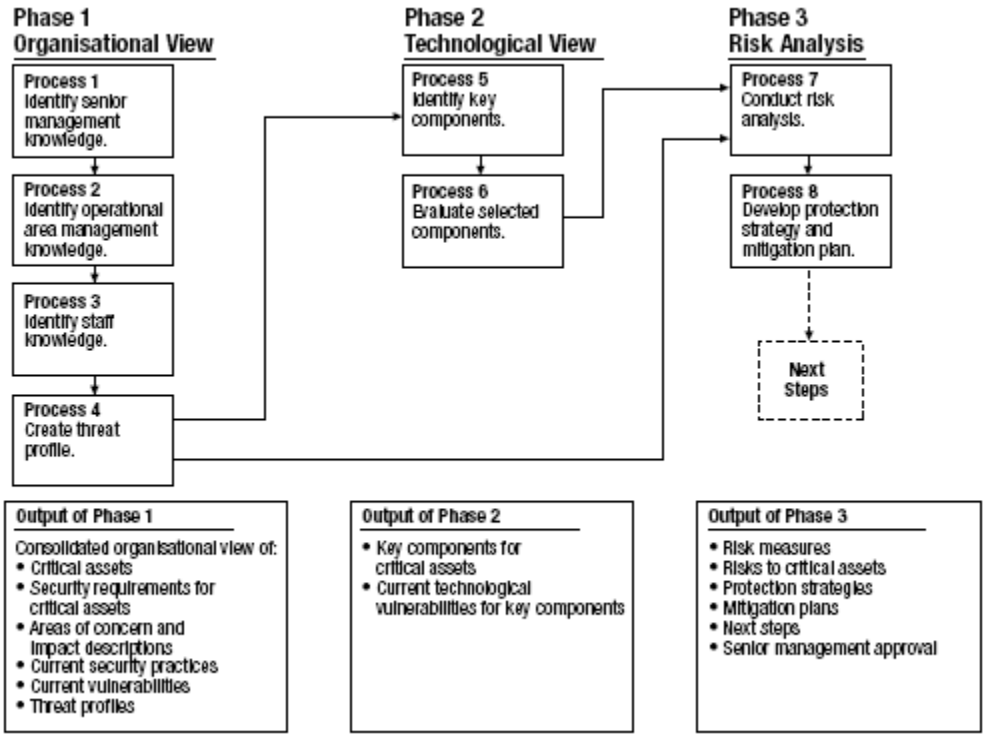

Figure 2.4:The OCTAVE Method (Panda 2009)

2.3.4.2 OCTAVE-S Method

This method is designed for small with flat hierarchical structures and less than 100 employees organizations in 2003. It uses the same three-phased approach of the OCTAVE method except that the processes are streamlined to four processes that meets the limited means and constraints of small organizations. It only requires a team of 3-5 organizational personnel who understand the organization's depth and breadth. The processes of OCTAVE-S are as shown in Figure 2.5.

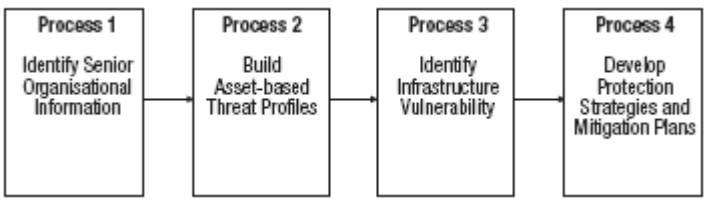

Figure 2.5: The OCTAVE-S (Panda 2009)

2.3.4.3 OCTAVE-Allegro Method

This method was designed to streamline ISRA so that sufficient results could be obtained with a little investment in people, time and other resources. It can be performed in a workshop-collaborative

setting. It is a streamlined variation of the above two methods. This method is easier to use, improves repeatability and reduce the technology view and the required training and knowledge. Although most organizations use OCTAVE-Allegro successfully, the two older methods are still available. The phases of OCTAVE-Allegro are as shown in Figure 2.6.

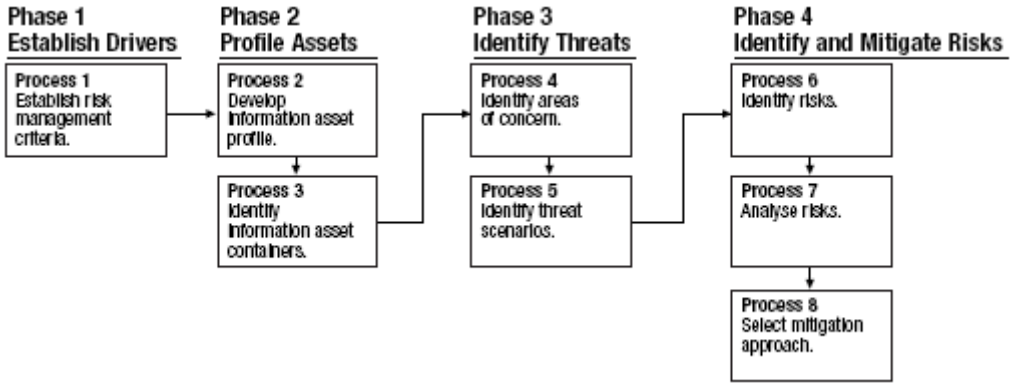

Figure 2.6: The OCTAVE-Allegro (Panda 2009)

Regardless of the chosen method, they are all self-directed where security needs are addressed by teams of organizational personnel, evolved where technology is addressed in a business context and builds an operational risk-based view of security and flexible where it is easy to tailor each method to the organization's needs.

OCTAVE is a qualitative methodology with threat-oriented analysis approach. It is a simple method where no mathematical computations are used. Just like CRAMM, OCTAVE does not include any steps regarding the implementation of security controls or follow up. Although OCTAVE is a lengthy method with many volumes, processes and worksheets, it is still yet flexible and has several methods designed for specific organizations. A major advantage of OCTAVE is that it is self-directed where it could be carried out by forming small teams from the organization’s personnel. Regardless of OCTAVE being a heavyweight methodology, it is widely used and has a lot of compatible third-party tools and supporting documentation (Panda 2009; OCTAVE 2014).

2.3.5 CORAS

"Construct a Platform for Risk Analysis of Security Critical Systems" is a methodology for ISRA developed under the European Information Society Technologies (IST) program (CORAS 2014). It is a self-contained model-based RA methodology that uses special diagrams inspired by Unified

Modelling Language (UML) to document intermediate results and to present the overall conclusions. The analysis is conducted in eight steps as follows:

Step 1: Preparation for The Analysis

The objective of this step is to get a general idea about the target and size of the analysis.

Step 2: Customer's Presentation of The Target

The objective of this step is to get an understanding of the customer's (organization) overall goals of the analysis and issues to be considered through introductory meetings with the required organization personnel.

Step 3: Refining The Target Description Using Asset Diagrams

The objective of this step is to ensure a common understanding of the analysis target, focus, scope and main assets to be protected through direct interaction with the customer (Rajabhandari 2013).

Step 4: Approval of The Target Description

The objective of this step is to ensure that the target, focus, scope and rest of the analysis are documented and are complete, correct and approved from the customer. A refined description of the analyzed target is described using the UML notation and a risk evaluation criteria is decided for each asset.

Step 5: Risk Identification Using Threat Diagrams

Risks are identified through structured brainstorming workshops of personnel from different organizational levels led by the analyst. In this step, threats, threat scenarios, undesirable incidents and vulnerabilities to the identified assets are systematically identified and documented through CORAS Threat Diagrams.

Step 6: Risk Estimation Using Threat Diagrams

The likelihood and consequences of undesirable incidents are estimated through brainstorming workshops of organizational personnel with different backgrounds. As a result, the risk level for each identified risk is determined.

Step 7: Risk Evaluation Using Risk Diagrams

Using the defined risk evaluation criteria and risk estimation results, all of the identified risks to assets or indirect assets are decided to be either acceptable or requires further evaluation for possible treatment.

Step 8: Risk Treatment Using Treatment Diagrams

Risk treatments to reduce the likelihood and/or consequences of undesirable incidents are evaluated and analyzed with respect to their cost-benefit. Finally, a plan for risk treatment is made.

CORAS is a model-based qualitative methodology with an asset/impact analysis approach. Furthermore, it has no steps for implementation of security controls and follow up. It is worth noting that CORAS can easily be implemented in organizations due to its simplicity. However, loss is not calculated using any mathematical functions but estimated by multiplying the probability of threat occurrence by impact. Thus, its risk analysis results cannot be precise (Bahattacharjee et al. 2012). CORAS is somehow a lengthy method where the first four steps are dedicated to defining and reaching an agreement among stakeholders on the target, context and goals of the RA. Whereas the actual RA is performed in steps 5 to 8. Although CORAS is no longer developed, it is comprehensive and has a free dedicated tool. One of the advantages of CORAS is that it facilitates continuous collaboration and communication between stakeholders. Nevertheless, it does require some expert knowledge.

2.3.6 ISRAM

Information Security Risk Analysis Method is developed by (Karabacak and Sogukpinar 2005). It is a poll-based quantitative RA method where the organization's staff and director participate in the analysis process. ISRAM established two separate investigation surveys for the risk attributes probability and consequence. To provide well-defined risks, the surveys flow and preparation are done in seven steps as shown in Figure 2.7.

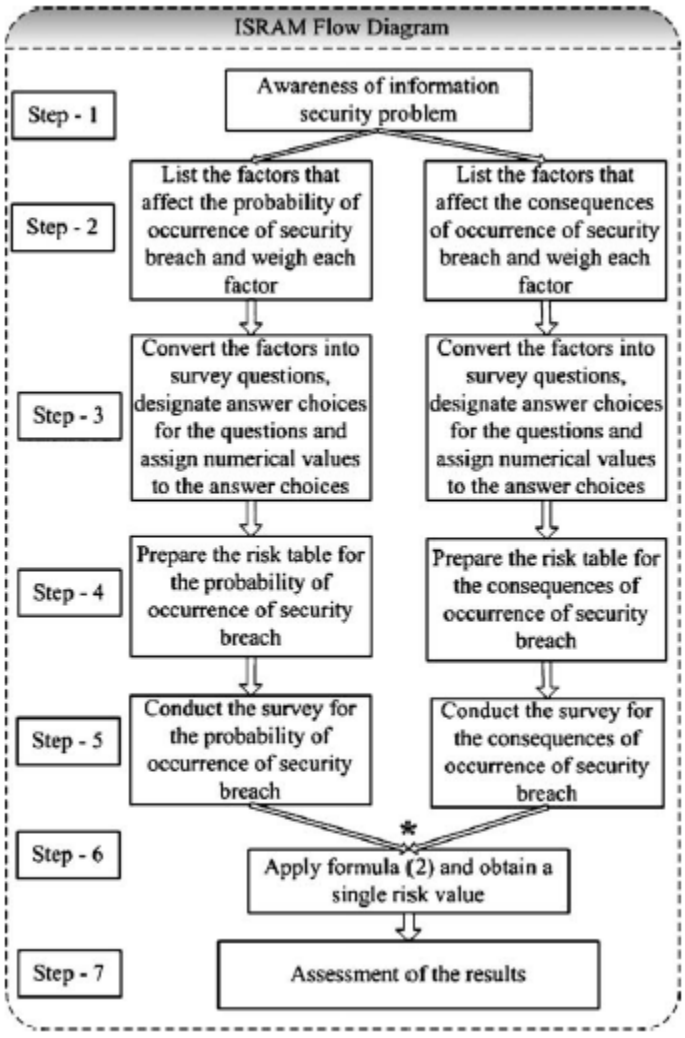

Figure 2.7: ISRAM Flow Diagram (Karabacak and Sogukpinar 2005)

ISRAM is a quantitative methodology with an analysis approach that can be set according to the type of given survey questions. It can be described as a "survey preparation and conduction process" for assessing organizations security risks. However, ISRAM relies on using public opinion of the information security problem by conducting a survey to make an as-is analysis. Furthermore, ISRAM is lengthy, where the first four out of seven steps are for the survey preparation phase. Although ISRAM is a quantitative methodology, there is no need to use complicated statistical and mathematical instruments. Organization's managers and staff could participate effectively in the RA process.

In conclusion, it can be seen that many methods have been proposed for ISRM in the literature. Although RA methodologies differ in their activities order and depth, they generally follow three distinct phases (Saleh and Alfantookh 2011; Shedden et al. 2011):

1- *Context establishment*: All the required information about the organization such as organization's strategy, structure, goals and current security status is gathered to ensure optimal RA results and that all related risks are identified.

2- *Risk identification*: Assets, threats to these assets and vulnerabilities that may be exploited by these threats are identified systematically.

3- *Risk analysis*: The probability of a threat (attack) occurring and its impact (cost) on assets are determined whether quantitatively, qualitatively or a combination of both. This will result in representing the risk level.

However, these methods are not equal. Some of these methods could be used as stand-alone RA methods while others need a low-level technical method to support the process of RA. Some of these methods are very generic and maybe used as guidelines to manage information security risks such as ISO/IEC 27005:2011. Furthermore, other standards provide an exemplary sequence of activities to conduct RA with a specific method for the determination of risk such as NIST SP800-30. Moreover, some methods such as CRAMM, OCTAVE and ISRAM do describe the process of RA at a high-level of granularity but do not suggest any steps regarding the implementation of required security measures or for follow up that should be considered. By contrast, some of these methods are designed for RM which incorporates RA. Thus, most methods follow a common process towards RA. Furthermore, more details are added after the analysis phase. A summary of the reviewed ISRM methodologies is shown in Table 2.1.

	Vendor	Country of origin	Official website	Assessment Approach	Analysis Approach	Skills needed	Compliance to IT standards
ISO/IEC 27005:2011	ISO	International	http://www.iso.org/	Qualitative/ Quantitative	Asset/Impact	Standard	ISO/IEC 27001
NIST SP 800-30	National Institute for Standards and Technology (NIST)	United States of America	http://www.csrc.nist.gov	Qualitative/ Quantitative	Depends on RA starting point	Standard	ISO/IEC 27001
CRAMM	Insight Consulting	United Kingdom	http://www.cramm.com	Qualitative	Asset/Impact	Specialist	ISO/IEC 27001
OCTAVE	Carnegie Mellon University, SEI (Software Engineering Institute)	United States of America	http://www.cert.org/octave/osig.html	Qualitative	Threat oriented	Standard	N/A
CORAS	European Commission	Greece, Germany and Norway	http://coras.sourceforge.net/	Qualitative	Asset/Impact	Standard	ISO 31000 ISO/IEC 27002
ISRAM	CNR Institute of Electronics and Cryptology and Gebze Institute of Technology	Turkey	N/A	Quantitative	Depends on RA starting point	Standard	NIST SP 800-30 ISO/IEC 27002 ISO/IEC 27005:2011

Table 2.1: Historical ISRM methodologies

According to reviews/surveys done by Wangen (2017), Gritzalis et al. (2018) and Yalcin and Kilic (2018), Table 2.2 represents the current status. Although HTRA was released in 2007, it has not been updated since. In 2011, CORAS was updated by adding up-to-date vulnerabilities, threats and safeguards. Since CRAMM's last update was in 2011, it is considered outdated. However, it is more up-to-date than HTRA. Similarly, EBIOS is considered outdated since it was released in 1995 and last updated in 2010. However, it is actively supported by a big organization, ANSSI. Compared to CRAMM and EBIOS, IT-Grundschutz is considered obsolete since it was released in 1997 and last updated in 2005. Many tools support IT-Grundschutz, but have not been updated since 2005. MEHARI is the most updated method since it was released in 1996 and last updated in 2017 (meharipedia 2019). The second most updated method is MAGERIT since it was released in 1997 and last updated in 2013. Furthermore, its supporting tools are continuously updated to comply with

current security demands and requirements. Although RiskSafe was released in 2012, it has not been updated. OCTAVE was first released in 1999 and last updated in 2005, whereas OCTAVE Allegro was released in 2007. To this end, MEHARI, MAGERIT, RiskSafe and CRAMM are methods which have been recently updated. Amongst them, CRAMM is considered as the most obsolete. However, CRAMM and its supporting tools have not received the same amount of updates in comparison with the other aforementioned methods. The ISO/IEC 27005:2011 was first released in 2011 but now it is withdrawn and revised as ISO/IEC 27005:2018 (International Organization for Standardization 2018). In terms of standards, ISO/IEC 27005:2018 is the most updated followed by NIST SP800-30. However, NIST SP800-30 is considered outdated since it was last updated in 2012.

	Method or Standard	Compliance with Standards	Type of Risk Model*	Release	Last Update
EBIOS	Method	ISO/IEC 27001, 15408-1:2009, 21827:2008	2	1995	2010
MEHARI	Method	ISO/IEC 27005:2011, 27001	1	1996	2017 (MEHARI Expert Knowledge Base)
OCTAVE	Method	N/A	4	1999	2005 (v2.0)
IT-Grundschutz	Method	ISO/IEC 27001	5	1997	2005 (v2.0)
MAGERIT	Method	ISO/IEC, 27002, 15408-1:2009, 27001	1	1997	2013 (v3.0)
CRAMM	Method	ISO/IEC 27001	1	1985	2011 (v5.1)
HTRA	Method	N/A	1	2007	2007 (TRA-1)
NIST SP800-30	Standard	ISO/IEC 27001	1	2002	2002 (rev.2012)
RiskSafe Assessment	Method	ISO/IEC 27001, HMG Security Policy Framework, The Baseline Control Set defined by HMG, PCI DSS, PSN Code of Connection, SANS Institute Top 20, Cloud Security Alliance's Cloud Controls Matrix	1	2012	2012 (v1.0)
CORAS	Method	ISO/IEC 27001, ISO 31000	5	2003	2011
ISO/IEC 27005:2011	Standard	ISO/IEC 27001	1	2011	2011 (rev. 2018 as ISO/IEC27005: 2018)

Table 2.2: ISRM Methodologies Current Status….. *As Discussed in Section 2.6

2.4 Enhancements to RA Methodologies

The main advantages of traditional RA methodologies (Tiganoaia 2012; Bergomi et al. 2013; Paul and Davillier 2014) are:

- Its compliance to standards allowing organizations to certify their risk management process.
- The ability to make informed decisions by comparing options and issues having measurements based on a systematic analysis of the problem.
- The existence of tools that could provide interfaces to other engineering tools.
- The seamless integration of risk management process with legacy engineering processes.

However, they do suffer from a number of disadvantages such as:

- Textual reports.
- Significant expertise
- Some issues of cognitive scalability.
- Different security experts can contribute over the years to the process in the case of long lived large systems.

Thus, there is a number of different proposed RA methodologies in the literature that are built on those methodologies where each method has its own objectives, steps, structure and level of application.

Moyo et al. (2013) performed an ISRM study to educate management and users of a computer information system (CIS) in secondary schools on how to protect their information assets and reduce risks to their information systems through risk management. Due to the lack of risk management experts within these schools, flat layered hierarchal structure and ease of use, the OCATVE-S methodology was adopted. It has been customized to fit the secondary schools risk environment and skill level. Risks were assessed using a qualitative risk matrix and treatment strategies were developed and implemented. It was found that an essential component of organizational ISRM is the security awareness and training of CIS users. The OCTAVE-s has been successfully applied in this study to identify an easy to use and simple RM methodology that can be used by Secondary Schools non-technical personnel. The authors have systematically collected data on information security controls

and critical assets in secondary Schools. Thus, they succeeded in defining general guidelines that could be easily followed during ISRM process having in mind that CIS users are not RM experts. Although the study was conducted in only three Secondary Schools (small sample size), the authors findings could be generalized to include CIS users of Elementary and Intermediate Schools due to the similarities in school's organizational architectures. However, given the conservative environment of schools, the observed behavior of the selected sample members maybe inaccurate with the presence of the researcher and may not reflect their actual normal behavior.

Bhattacharjee et al. (2013) proposed a two phase quantitative ISRA methodology for organizations that comply with the requirements of ISO/IEC 27005:2011. Two approaches, a consolidated and a detailed, were proposed to risk identification. In the consolidated approach, which should be carried out first, an asset is in a high, medium or low risk zone depending on its computed risk factor value that is between 1 and 5.

Risk factor = f (asset value, security concern),

where the asset value is a function of security in terms of CIA, authentication and non-repudiation, legal and business (in terms of loss impact) requirements associated with an asset. The Security concern is defined to be a function of threats and vulnerabilities of an asset.

A detailed risk analysis, *the detailed approach*, will be carried out for assets that are in the high or medium risk zone to identify threats and vulnerabilities that cause these threats. The risk value will be computed as:

Risk = f (security requirement, threat, vulnerability, risk value),

where risk value is computed in terms of the security requirements value, the likelihood of a threat and severity of a vulnerability. As a result, assets are classified into High risk assets (danger zone) which has to be mitigated, Medium risk assets (warning zone) that should be controlled by applying security policies and guidelines and implementation of security tools. Low risk assets (safe zone) are accepted risks where no investments are made. This proposed methodology is threat-based, the same as the OCTAVE methodology. However, it is better than the OCTAVE method because the asset value is formally computed with regards to security, business and legal requirements.

Theoharidou et al. (2012) proposed a RA methodology for smartphones that has an ISO/IEC 27005:2011 compatible theoretical basis. Current RA methods are not for users but for businesses and treats smartphones as a single entity without any consideration of the smartphone security model vulnerabilities and smartphone specific threats. The proposed RA method divides the smartphone into a number of sub assets, then smartphone specific threats are assessed. The authors classified smartphone assets as Device, applications, connectivity channels and data. The data asset is classified according to two dimensions, information type and source. First, asset impact is assessed then smartphone assets are related to different smartphone specific threat scenarios. The user is involved in the initial process of impact valuation. The overall risk is calculated by the risk analyst. To calculate the total impact valuation, the maximum impact from all smartphone-identified assets is the overall smartphone impact. Risk assessment is calculated on the basis of a risk matrix as Low, Medium or High. The authors demonstrated the proposed RA method in the Android platform. The proposed risk assessment method provides "fined-grained" valuation. The authors proposed risk triplets where they use application permissions as the attack vector, associating assets to threats and permissions combinations. Risk is, then, assessed as a combination of asset impact and threat likelihood. User input for (sub)asset impact is based on a two-dimensional data taxonomy. This user involvement, leads to a 'personalized' risk assessment, where other smartphone oriented methods mainly use expert opinion. However, user input details vary according to user skill which may affect the quality of results. Also, users assessing the asset impact of application is complex where the number of applications maybe numerous and the user is assumed to know the applications significance. The proposed method has been tested in a hypothetical case study, so no strong indications on its effectiveness.

Gros (2011) argues that RA relies on the risk assessors expertise which results in an error prone and tedious process that may not reflect the real situation. By treating information systems as complex systems that has interconnecting components, a risk management methodology was proposed based on NIST SP 800-30 risk management guide. Complex systems are systems that have an internal structure, uncertainty, evolves and adapts to inputs and has a non-observed behavior in its basic parts.

Supply chains, The Internet, traffic systems are all examples of complex systems. In the proposed method, all resources are enumerated and connections are built between them, where resources values are measured independently of any subjective opinion. Two methods are used to get the final values of all other resources depending on it. Then, threats, vulnerabilities and controls for all resources are added. Security risks are analyzed where they are by analyzing how threats can spread through the system. Depending on decisions by management, controls are added to accept or lower the highest risks. The model is improved by adding more details to it, i.e. connections, resources and controls. RA is done by evaluating probabilities and ways that threat sources get to each information system component. However, the proposed methodology does not determine the exact interaction between controls and resource dependency nor evaluate the way in which threats spread through the system.

Samy et al. (2010) were motivated by some facts about most existing risk management methods such as:

- The estimation of the probability of an identified vulnerability mainly on "guesswork or rough estimation" due to unreported cases or missing (censored) information.
- Identification of threats by using horizontal data with a static timeframe.

As a result of this inaccurate information, decision makers will make wrong decisions on information security and waste their time and effort on controlling the wrong things. Thus, the authors adopted the survival analysis approach, namely the Cox Proportional Hazards PH Model, to identify potential information security threats. The authors proposed integrated framework is as in Figure 2.8.

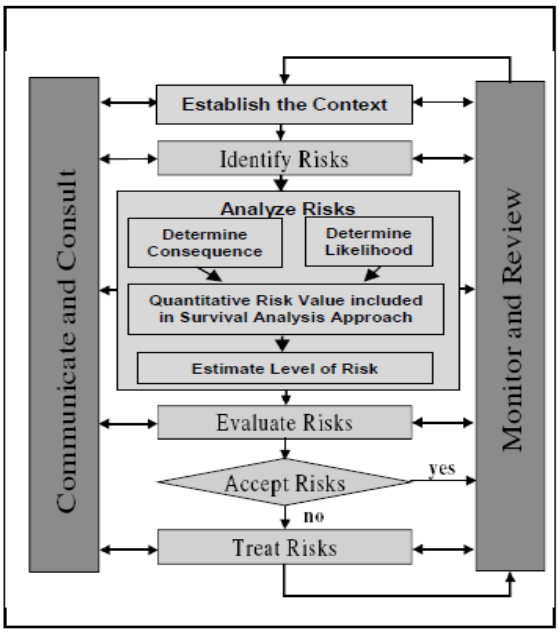

Figure 2.8: Adoptions of Survival Analysis approach in Risk Management process framework (Samy et al. 2010)

The authors used a qualitative approach, structured interviews, to identify potential threats then a quantitative approach, survival analysis, to analyze the risks. Then, the authors adopted a follow-up study to analyze and collect the lifetime of the systems i.e. start and failure time according to predefined analysis periods. The proposed framework can be used in organizations that suffer from a lack of appropriate data to undertake ISRA. A particular strength of this framework is that it considers the time dimension in identifying threats that vary over time. The study highlights some of the deficiencies that were mentioned in (Webb et al. 2014). The proposed framework is built on the standard AS/NZS 4360:1999, the authors offered no explanation why. There could be difficulties with applying this framework in practice since it has not been tested yet, so no indications of its effectiveness and reliability.

Regardless of the various published risk management methods and standards, organizations either fully or partially adopt such standards and methods to manage risks in their IT activities. It is more convenient to have a well-designed comprehensive method that supports ISRM compatibility among organizations and accommodates the different requirements of such methods. Saleh and Alfantookh (2011) proposed a comprehensive framework for enterprise ISRM. The frameworks is composed of two parts, structural and procedural:

- *The Structural view*: The scope dimension is based on the five STOPE domains of Strategy, Technology, Organization, People and Environment.

- *The procedural view*: the process dimension has the five cyclic phase of six-sigma model DMAIC, Define, Measure, Analyze, Improve and Control.

The authors use of STOPE in their framework makes it able to accommodate different current or emerging ISRM issues. The use of six-sigma DMAIC processes allows the proposed framework to accommodate processes of other ISRM methods in one unified process. However, the proposed framework has not been validated or tested yet. It is theoretically considered to be of flexible nature which makes it an "open-reference" for ISRM that can be used by enterprises.

Bergomi et al. (2013) used the CORAS methodology to integrate a model based ISRA view to the mainstream engineering views of complex software-intensive information systems architecture description. This was done to maintain traceability, implementation and use of relationships between design artifacts and security artifacts. As risks are identified, they are documented using CORAS threat diagrams that build up the risk model. These threat diagrams model threats, vulnerabilities, threat scenarios, harmed information assets and unwanted incidents. CORAS supports traceability techniques to maintain consistency between the risk model and the system model. The Risk Monitor of the CORAS tool is used to continuously update risk estimation by monitoring key risk indicators i.e. threats, vulnerabilities, threat scenarios etc.

Nevertheless, various RA techniques whether qualitative, quantitative or semi quantitative have been used in the literature to assess and analyze information security risks such as HAZOP, fault tree analysis, cause and effect analysis, Bayesian networks and decision trees (Alguliev et al. 2009; Sadiq et al. 2010; Tao et al. 2010; Pirzadeh and Jonsson 2011; Poolsappasit et al. 2012; Imamverdiyev 2013; Tamjidyamcholo et al. 2013;). The chosen risk technique should meet the study objectives, decision maker's needs, the analyzed risk types and consequences magnitude. However, the selection of such technique depends on several factors such as resource availability, degree of uncertainty and complexity of analyzed system (ISO 2009).

However, despite the increased attention on Information Security Risk Management (ISRM), there is a lack of research on the effectiveness of RA practices and implementations in organizations compared to research on ISRM theory, method and concepts. This was due to the reluctant behavior of organizations to discuss their Information security practices and that such investigations require knowledge of information systems and risk management. This lead to the following deficiencies in the practice of ISRA:

1- The identification of information security risks is perfunctory, where significant risk sources such as risks related to intangible assets, early indications of malicious threats and vulnerabilities found in relationships between information assets were not considered during the Risk Management (RM) process.

2- Little reference is given to the organization's situation when Information security risks are estimated.

3- ISRA is done on a non-historical, intermittent basis where information gathered at any time represents a "snapshot" of the organization's Information security environment (Webb et al. 2014).

In addition, there exists some problems in the current ISRA approaches such as:

1- How uncertainty in risk estimation is handled and the lack of estimation data.

2- The extensive focus on the protection of physical assets.

3- Lack of appropriate risk identification and communication methods (Paintsil 2012).

2.5 ISRM for the general public

The high cost of information security is not only in the price of the application itself, but in convincing users to adopt security measures (Jain and Clarke 2010; Alawadeh and Tubaishat 2014; Webb et al. 2014). Even when these measures are applied, it is found that users have great difficulties in using, understanding and reacting to these applications and potential threats. Users awareness of information security risks is fundamental to effective information systems security (Zabaa et al. 2011; Komatsu et al. 2013).

According to Jain and Clarke (2010), there are some websites that provide information and advice on how to protect yourself in the cyber world such as Getsafeonline.org and Staysafeonline.org. However, these could be used as awareness tools that provide advice and guidance to users regarding their security behavior. They do not provide the expected level of RA that users are exposed to. Hence, we can conclude from the above that there is a lack of tools and methods for Information Security Risk Assessment (ISRA) in the literature that are tailored for the general public. This is in contrast to the increased attention on ISRA in enterprise organizations (Sulaman et al. 2013; Webb et al. 2014).

With the increase use of broadband Internet by home users, this exposes them to potential security threats and unauthorized access to information, systems and resources. Many of these home users are not aware of these risks and/or do not have the necessary knowledge to use the available websites to analyze these risks and overcome security risks problem. Jain and Clarke (2010) proposed a web-based risk analysis tool for home users based on the ISO 17799 standard, where only sections that are relevant to home users were used. The proposed tool followed a three-process risk management strategy to analyze, mitigate and evaluate the risks. The authors used a quantitative approach to analyze the risks. In the analysis process, assets and threats to these assets are identified. In this quantitative approach, risk level is calculated as high, medium and low which is fairly understood by home users regardless of their information security background. The ISO 17799 controls that are applicable to the home user were used by the authors to assess the risks by allowing the user to answer some proposed questions. The authors identified a number of threats to home users and quantified their probability and potential impact. At the end of the risk assessment, the risk level value of each of the seven ISO 17799 derived categories is displayed to the user as HIGH (100), MEDIUM (50) and LOW (10) with the required support. However, the tool was tested with only 20 participants (a very small number of participants) without any information given on their information security background. Thus, the performance of the tool was evaluated with means of the interface design described as user-friendly, easy to use and accessible. No evaluation regarding the way the tool

assessed the different security levels and the provided support, maybe because it has not been tested by users with a certain level of security background.

Ledermuller and Clarke (2011) proposed a Mobile Device Risk Assessment (MDRA) risk assessment method based on a 6-step risk calculation scheme where risk levels are determined using the standard risk calculation formula

Risk score = asset * threat * vulnerability

Due to the increasing number of available apps, bespoke apps that might exist and lack of research on threats and vulnerabilities in the mobile context, the authors proposed categorization to determine the asset value and threat. Categorization of asset values was based on trends of mobile phone usage and market offers (Apple App store, Blackberry App World … etc). Threat categories were developed from literature. However, vulnerability level was determined by answering a list of proposed T/F questions based on the SANS top software errors.

The proposed MDRA operates in private, corporate and hybrid contexts and consists of three main stages, operator, corporate and private. To define the default risk scores, the network operator has to perform the RA process for each category. The second stage is performed by the organization only if the device is used to access or store company information. The organization can store their RA settings after conducting their RA. In the third stage, the user has to choose his knowledge level when using MDRA for the first time. All other steps are automated. The authors developed a prototype of the proposed methodology and the prototype screens were used to conduct a preliminary physical trial of thirteen participants with different knowledge levels. The authors found that most participants knew that there is valuable information stored on their devices. However, the whole risk calculation process was challenging for novice users which resulted in them using the application in a passive way as an information source with no intention of changing values. Other users tend to use it in a more active way (changing values). The proposed approach is clear and easy to use by different stakeholders other than novice users. However, the approach is mainly based on the assumption that network operators will provide the default values by performing first instance Risk assessment. Allowing other stakeholders such as security vendors to provide such values then having a mechanism

to calculate the default scores based on values provided by network operators and other interested stakeholders might result in more realistic default value scores. The approach has not been really tested, participants judged the application according to screenshots of what an application might look like which may have resulted in weak indications. Due to the small number of participants, 13 only, and them not having the ability to test the prototype on their mobile devices, the obtained results may not actually reflect the usability, friendliness and robustness of this application to suit the general public.

To help general users understand mobile applications security risks and to provide a technique that continuously and automatically assess information security risks of Android mobile applications, Jing et al. (2014) proposed a continuous and automated risk assessment framework for Android mobile applications called RiskMon. The main idea of RiskMon is to use machine-learned ranking to assess risks. RiskMon creates a baseline from users expectations and behavior of trusted applications. Then, baseline assigns a risk score to an application whenever it attempts to access sensitive information through assessing API calls. Applications are ranked based on their accumulative risk score. The proposed framework represents a technique to reveal suspicious behaviors of Android mobile applications. It is different in a way that it provides continuous and automated risk assessment based on the installed application's behavior. Although, users specifying security requirements for security tools is a challenging task, the framework design allows for user's expected behavior rather than developers practices. However, it is subjective since it relies on user's input of relevancy levels for permission groups (user's expectations) and their understanding of these permission groups for each trusted application. This may result in biased choices. It also uses information from the applications market which is an advantage of this framework. However, the use of number of reviews regardless of what they are and who wrote them is a major drawback. Users may simply choose not to use this RiskMon, due to the long time required to set relevancy levels – set by authors as 5 to 10 minutes for 10 applications. This may be considered as a usability overhead.

Users are facing difficulties in adequately securing themselves (Van Cleef 2010; Mensch and Wilkie 2011; , Zabaa et al. 2011; Komatsu et al. 2013; Mylonas et al. 2013; Webb et al. 2014). Even

with the mix of awareness programs and legal and technical measures, users can not well-protect their privacy on social network sites (Van Cleef 2010; Mensch and Wilkie 2011; Mylonas et al. 2013; Li et al. 2016; Mendel et al. 2017; Liu et al. 2018). Users use social media for many purposes such as using Facebook to share posts with family and friends, Instagram to share pictures and Twitter for microblogging. Unfortunately, some users are less concerned about information privacy; therefore, they post more sensitive information without specifying appropriate privacy settings. This could be due to them not being aware of how to do it or simply because they do not see their personal data, such as sharing their locations, as an attractive target to compromise (Adelola et al. 2015; Yu et al. 2018). Therefore, over-sharing and disclosing of personal information, whether intentionally or unintentionally, may result in exposing them to security risks they are not arguably well-aware of such as social engineering and phishing (Tayouri 2015; Laleh et al. 2018). With regards to privacy protection of social networks users, most privacy protection techniques focus on mechanisms such as access control (Pang et al. 2014; Daud et al. 2016) and anonymization (Fard et al. 2015; Liu et al. 2018) and assuming that they can be adopted by users. However, the growing number of security incidents and vast amounts of disclosed personal information raises the question on how to best motivate/educate users to protect themselves. Actually, as a reaction to some data breaches, media attention and privacy awareness campaigns may have resulted in users being alerted to the term "privacy". One recent incident, early 2018, is the Facebook-Cambridge Analytica data breach. This happened when Facebook allowed its data mining partner, Cambridge Analytica, to harvest the personal data of millions of Facbeook users without user's express consent and used it for political purposes urging the need for greater user protection and the right to privacy (The Cambridge Analytica Files 2019).

Motivated by the fact that users need a security process to deal with security risks they face, Van Cleef (2010) suggests that users should be held responsible and in control of their own devices, data and services. He proposed a Personal Chief Security Officer (PCSO) tool to help users in managing Info Sec risks. PCSO has four components:

- *Personal user interface* that gathers information from all systems and applications used by the user and displays it on the dashboard along with information about risk exposure. Also, information about CIA and residual risk are displayed. A wizard configures the user's security process. Information about ISRM is stored in a personal database along with user's goals, owned IT systems, performed tasks and tasks that has to be performed by the user to manage risks. The user is contacted at regular intervals, through a scheduler, to assess any changes that need to be considered.
- *Shared risk repository* where frequently used data that users do not have to enter themselves such as security goals, software categories and attacks are stored. It is maintained collaboratively by security researchers, users and enterprises.
- *Interoperability module* that links other tools and applications to PSCO to make the risk management process easier and faster.
- *Risk communication module* that shares the ISRA results between users.

Although many parts of this tool already exist and can be adapted by users, no indications on the efficiency, feasibility and ease of use of this tool. However, the idea of making the user assess risks for all his devices and data in one tool is interesting and maybe appealing to him. This may have a positive impact on his security behavior since it saves the time and effort by securing all his devices form one tool. Thus, this tool may act as an awareness precondition.

2.6 Discussion

Most RA methodologies analyze risk based on an asset/threat relationship where risk is determined using the classic interpretation of risk

$$\text{Risk} = \text{Asset} * \text{Threat} * \text{Vulnerability}$$

Although RA methodologies differ in the RA starting point, how risks are treated in similar threat scenarios and assessment detail, this asset/threat relationship can be analyzed in many ways. Thus, a similar list of critical assets may be found in many organizations whereas threats to these assets may vary according to the organization's Information security scope (Shamala et al. 2013).

Based on whether risk is evaluated quantitatively or qualitatively, which factors are considered when impact is evaluated and how these factors are combined to calculate risk, Zambon and Etalle (2011) presented five types of risk models as follows:

Type 1:

*Risk (Threat, Asset) = Likelihood (Threat) * Vulnerability (Threat, Asset) * Impact (Threat, Asset)*

Type 2:

*Risk (Threat, Asset, Security Requirements) = Impact (Threat, Security Requirements) * Vulnerability (Threat, Asset)*

Type 3:

*Risk (Threat, Asset) = Annual Loss Expectancy (Threat, Asset) = Probability (Threat, Asset) * Average Loss (Threat, Asset)*

Type 4:

*Risk (Threat, Critical Asset) = Impact (Threat, Critical Asset) * Vulnerability (Critical Asset)*

Type 5:

*Risk (Incident, Asset) = Likelihood (Incident) * Consequences (Incident, Asset)*

In RA methodologies that use Type 1 risk model, such as CRAMM, ISO 27005:2011 and NIST SP 800-30, risk is evaluated as the combination of the likelihood that a certain threat will attack on an asset, the vulnerability (exploitability) of an asset to the threat and the potential impact of that threat on the asset. This is the classic interpretation of risk that is used in most general-purpose RA methodologies. In these RA methodologies, risk is computed as the likelihood of a threat attacking an asset(s) and the impact that successful attack (threat) has on an asset(s). The vulnerability level of an asset(s) to the threat is considered implicitly as one of the likelihood factors.

In organizations where security requirements have to be defined before-hand, RA methodologies that use Type 2 risk model could be used where risk is analyzed with respect to both asset/threat relationship and security requirements. Risk is assessed basically on the impact that a threat has on assets security requirements and the vulnerability of these assets to threats. These kinds of

methodologies follow the top-bottom approach represented by (Paintsil 2012), where the security needs of an organization are based on the security requirements for CIA and risk to legal, infrastructure and regulatory requirements. The required security level of an organization is determined by the security needs. Accordingly, risk is interpreted as a violation of a security requirement. Whereas other RA methodologies follow the bottom-top approach where risk is assessed by identifying asset, asset value, the likelihood of an incident and its consequences. However, the likelihood of a threat attacking an asset is not considered in type2 RA methodologies. This type is most suitable if the purpose of RA is for certification.

For some quantitative RA methodologies that require quantitative data, risk is interpreted financially (in monetary value). It is calculated for each asset/threat as the annual loss expectancy. In these Type 3 risk model RA methodologies, a time frame (yearly) is used explicitly in analyzing risk. Furthermore, risk is calculated as the probability of a threat affecting an asset in a one-year time frame and the resulting average loss. These RA methodologies are most applicable in cases where decisions are made based on cost/benefit analysis.

RA methodologies that use Type 4 risk model, such as OCTAVE, a variation to the classic risk model is used. In these methodologies, critical assets are identified. These assets should be totally protected at all times against all kinds of threats. Hence, the likelihood of a threat attacking an asset is irrelevant in computing risk. Therefore, the impact of a threat successfully exploiting a vulnerability in an asset is combined with the vulnerability of this critical asset in order to compute risk. These kinds of methodologies could be used in assessing risks of security-critical systems such as in air traffic control systems, medical systems and utility network infrastructure.

Type 5 risk model RA methodologies, such as CORAS and ISRAM, do not take into account specific threats and focus only on system's weaknesses. Hence, risk is analyzed with respect to an incident, i.e. a threat exploiting a vulnerability, and an asset. The consequences of such incidents are combined with their likelihood in order to evaluate risk. Therefore, risk can only exist if a threat exploits a vulnerability or a set of vulnerabilities. These RA methodologies are more fine-grained and

different from Type 1 because they focus on system's weaknesses rather than a threat attacking an asset even without the case of an existing vulnerability.

It can be implied that variations and differences in RA methodologies and how risk is calculated are due to several reasons:

1. The meaning of risk to an organization and how it is interpreted.
2. The relationship between risk factors and their meaning.
3. The way risk factors are measured and computed in order to calculate (whether quantitatively or qualitatively) risk.

However, despite the different names that are used for the same factor or concept, the factors Asset, Threat and Vulnerability are found in all RA methodologies. Furthermore, most RA methodologies determine the risk level by multiplying Impact by Likelihood. The difference is in how they are decomposed and estimated. Moreover, there is no explicit differentiation between probability, i.e. 'how likely' an event to occur, and frequency of occurrence, i.e. 'how often' an event occurs, when analyzing risks. Furthermore, the vulnerability of an asset to a threat is not considered explicitly but implicitly as one of the likelihood factors. Vulnerability aspects, such as level of exploitability, the severity and propagation of a vulnerability over time are arguably not adequately considered. For example, the likelihood (probability) factor may be estimated by comparing the system with a known standard or based on empirical data found in similar context or on the subjective assessor's experience. Thus, there might be a big difference between a correct probability and an estimated probability, i.e. uncertainty in estimated risk, due to the lack of data on future events, new risks and vulnerabilities. This uncertainty about specific risk factors values may result in uncertainty in RA results. To our knowledge, little research has been made on how to compute this uncertainty. However, the degree of this uncertainty may be represented by expressing RA results qualitatively where a range of values are provided for identified risks rather than a single value or by using fuzzy regions to represent these results (ISO 2012).

One of the problems of current RA methodologies is that there are no fixed standards on how to develop lists of threats, vulnerabilities and risk levels. This may result in subjective unsatisfactory RA

results due to the reliance on stakeholder or risk assessor's experience. Thus, one way to reduce personal experience differences and work and analysis time is by using automated RA tools such as CRAMM, CORAS and OCTAVE (Panda 2009; Yazar 2011; CORAS 2014).

Furthermore, it is difficult to value assets accurately. Assets could be tangible, intangible and located in distributed environments. Due to the fact that risk occurs in a continuously evolving distributed and dynamic environment, it is difficult to determine the completeness and correctness of identified assets, threats and vulnerabilities. However, risk estimation maybe simplified by isolating interconnected events which may have a negative effect on the RA results reliability (Zambon and Etalle 2011; Bhattacharjee et al. 2013).

Current RA methodologies fail to comprehensively identify inter-asset relationships, relationships between threats and vulnerabilities and dependencies among vulnerabilities. The dependencies among risk elements are not properly addressed where each method is suited to a particular enterprise. Eventually, this results in an inaccurate and incomplete RA results that either over or under estimate risks. Bhattacharjee et al. (2013) proposed an asset-based RA methodology that considers these aspects when risk is computed. They reformulated their methodology in (Bhattacharjee et al. 2012) to formally model dependencies between assets, threats and vulnerabilities. Furthermore, all risk elements are formally modeled including vulnerability severity and exploitability. Considering the fact that a vulnerability could propagate through risk factors casual chains resulting in different risks, Feng et al. (2014) proposed a risk analysis model that identifies the casual relationships among risk factors using a Bayesian Network. Then, to determine the highest probability and the highest estimated value of risk, an analysis of vulnerability propagation is performed. Although these methods present, to some extent, a way of handling the uncertainty in assessing risks and relationships among risk factors, they are found to be complex, lengthy, require certain experience to implement them and lack tool support. However, the organization's actual risk scenario nor the uncertainty in risk factors are not properly represented.

Most RA methodologies are static, i.e. time is not included explicitly in calculating risk. They are found to be ambiguous, imprecise and cannot effectively communicate the system's dynamic behavior, adversaries and actors to system stakeholders. Threats and vulnerabilities that vary overtime are identified using horizontal data with static time frame (Sadiq et al. 2010). There is a need for a dynamic Information security RA model that considers the time dimension and continuously provide an updated probability. Although the risk model presented by Jing et al. (2014) provides a continuous and automated RA, it is considered as low (machine)-level and limited to Android Mobile Apps.

Moreover, current RA methodologies do not consider relationships among risks where if one risk occurs, then another risk is less or more likely to occur. These relationships might decrease or increase the likelihood of a specific risk occurring. In this case, these risks can be coupled so that several low-level risks may be combined into a higher-level risk. Hence, these relationships can be realized if several risks occur concurrently or when the same risk occurs repeatedly over a certain period of time.

Since the scope of this research is to develop a novel RA methodology for users of the general public and from the discussion above, it can be implied that there is a need for a well-structured and systematic process that can:

- Properly and explicitly identify important risk factors and contributors to security risks and thus reduce the impact of the important contributors. Relationships and dependencies between assets, threats, vulnerabilities and risks should be considered.
- Perform a dynamic RA of the risks the users are exposed to. Hence, it has to provide, to some extent, a continuously updated impact/probability and their deriving factors. Thus, whenever there is an available new information such as additional assets and changes in threats\vulnerabilities, it should be incorporated to update previous estimations. This information could be obtained from a real-time community based database.
- Consider if any security controls are taken into account in advance. If so, then the effectiveness of such controls should be assessed.

- Adapt to the user's level of security background and communicate RA results accordingly in a simplified and understood way. Furthermore, users are encouraged to make informed decisions by giving recommendations on what to do.
- Employ a requirement-oriented approach to RA instead of the classic asset-oriented approach used by most current RA methodologies. The user's security requirements are established before-hand and therefore the required security level will be determined accordingly.
- Reduce the uncertainty in the process of RA.

2.7 Conclusion

There are various ISRM methodologies whether quantitative, qualitative or semi quantitative. They all have the same goal which is to estimate the overall risk value. The majority of such tools and methodologies are tailored for organizations. ISRM is expensive, time consuming and depends on the expertise of risk assessors. There is no exact risk value. Although Risk maybe quantified, the uncertainty in defining severity of consequences and likelihood makes RA complex and subjective. To overcome this, a number of techniques were recommended to analyze risks and to make the ISRM to some extent error prone.

Although these methodologies have contributed significantly to current knowledge, little attempt has been made to assess risks for the general public. Thus, those tools and methodologies either are too difficult to be used or understood by users or they could be used as an awareness tool with no guidance offered to users to make informed decisions. Moreover, a gap is found in the literature in assessing risks for users of the general public where little research is found about tools and methodologies tailored for them. This implies that a structured approach tailored for users of the general public is needed. Additionally, user's awareness of such security risks and what influences their risk-taking behavior is a step forward in helping them assess and analyze the risks they are exposed to.

Chapter 3 : Information Security Awareness for the General Public

3.1 Introduction

A decade ago, information security literature overlooked the human aspect and focused upon the technological aspects and that security technology will provide the required level of protection against information security threats (Ophoff and Robinson 2014; Alotaibi et al. 2017). However, technology alone have been found not enough to ensure the CIA of assets as it can be misused by users and become vulnerable to various threats and, thus, losing its usefulness (Furnell and Clarke 2012; Kaur and Mustafa 2013). Indeed, users have problems in understanding both basic and advanced security options of some security technologies and standard tools (Furnell and Moore 2014). However, there is no security technology that is free from user-centric flaws such as opening an email attachment without checking and usability problems with security software interface (Bostan and Akman 2013).

The protection of various information assets, in an organizational context for example, mainly depends on several aspects such as the successful development and application of security plans, procedures and guidelines where the implementation of various information security controls as well as the consideration of the human aspect of information security are parts of it. This human aspect is directly related to knowledge, i.e. what users know, attitude, i.e. what users think, and behavior, i.e. what users do (Alarifi et al. 2012; Kaur and Mustafa 2013). However, before the implementation of such plans, guidelines and good practices, there has to be an appropriate level of Information Security Awareness (ISA) among users where they are aware of the potential information security risks and appreciate the need for protection against information security threats. Information security threats can be classified, broadly, to:

- **Physical threats**: These are mainly caused by threats such as natural disasters and physical theft of device. These threats could be mitigated by making multiple copies of information on a regular basis and storing them in widely dispersed locations or by using remote data wipe as in the case of smart phone theft (Mylonas et al. 2013; Ophoff and Robinson 2014).
- **Non-Physical threats**: These are mainly caused by humans such as malware, social engineering and phishing attacks. These are considered to pose the greatest risk due to the

changing and sophisticated mechanisms in conducting such attacks. Whereas, to allow such an attack, they usually target the weakest link in information security and exploit user ISA vulnerability. Indeed, most of these attacks cannot be detected by technology only and requires a level of awareness of what they look like and how to protect against them.

Attackers are continuously increasing their efforts to develop advanced and sophisticated hacking methods and malware that can be used to steal information and money from users (Aloul 2010; Hasan and Hussin 2010; Sheng et al. 2010). During 2017, 29.4% of user computers around the world were subjected to at least one attack compared to 31.9% in 2016 (Kaspersky 2017). While the Internet is still the main source of malware in most countries, this decrease may be due to several reasons such as Federal laws introduced and enforced by Governments worldwide to fight against cybercrime (Aloul 2010), search engines and web browsers are becoming more secure against malicious sites (Kaspersky 2017) or simply because Internet use in some countries, such as South Africa, is not highly developed (Ophoff and Robinson 2014). Nevertheless, attacks still occur. This could be due to lack or limited enforcement of cybercrime laws in some countries especially in the Middle East, lack of the existence of such laws among residents of such countries and the arguably limited ISA among users (Aloul 2010; Al-Hadadi and Al Shihani 2013). Further to that, security experts are issuing warnings of the emergence of newly designed malware that avoids detection and removal (Martin and Rice 2011). Attackers have a guaranteed chance to infect the user's computer with malware if it has at least one vulnerable, not updated and popular installed application (Kaspersky 2017). However, one way to mitigate these attacks and reduce their severity is by raising the Information Security Awareness (ISA) level of users (Aloul 2010; Alarifi et al. 2012; Furnell and Rajendran 2012; Al-Hadadi and Al Shihani 2013).

ISA is regarded as one of the significant defense lines against the continuously evolving information security threat landscape where a high level of ISA and practice can increase the performance efficiency of information security controls and, accordingly, decrease information security risks (Alarifi et al. 2012; Furnell and Clarke 2012; Furnell and Moore 2014). This implies that whenever humans are involved in an information security process, then users need to understand

their responsibility in the need to gain the required level of awareness of their information security related role and how to protect themselves (Kritzinger and von Solms 2010; Kritzinger and Von Solms 2013).

Home Users (HU) are citizens with varying technical knowledge and age who use Information and Computer Technology (ICT) outside their work environment for personal use (ENISA 2010). The terms HU, users or users of the general public will be used interchangeably to refer to this kind of users. Those users are solely responsible for the protection of their own devices and information. However, little evidence is found that they are knowledgeable of information security threats, how to protect against them and actually practicing it (Talib et al. 2010; Rao and Pati 2012; Kritzinger and Von Solms 2013). This is evident as they lack ISA in general, do not keep up to date with knowledge about new security related technologies and risks and use inadequate or incorrect security protection, if any. This explains why they tend to use weak passwords, do not set correct security settings and forget to update their software (Alarifi et al. 2012; Rao and Pati 2012; Kritzinger and Von Solms 2013). This ill-informed behavior makes them vulnerable to an increasing number of security threats such as Operating System vulnerabilities, Virus (malware) attacks, privacy violation and identity theft and spyware (Alarifi et al. 2012; Kritzinger and Von Solms 2013; Furnell and Moore 2014). Further to that, they perceive their lack of knowledge as one of the obstacles in achieving protection (Furnell et al. 2008; Wash and Rader 2011; Rao and Pati 2012). As a result, they try to delegate this security responsibility to technology such as Firewalls and Anti-Virus software, to another person or IT staff, to some institution like a Bank or simply ask for advice from family and friends rather than asking for formal support from official websites and experts (Furnell et al. 2008; Wash and Rader 2011; Furnell and Moore 2014). Nevertheless, they are still needed to make some security related decisions on a regular basis (Furnell and Clarke 2012; Harbach et al. 2014).

Educating users about information security threats is a challenging but a must to fight against these threats especially that security is considered a secondary task and not a primary task for them. Actually, reading technical material or playing an educational security game to increase their

information security knowledge may not be what they like to do in their spare time. This may be due to lack of resources, time, motivation and learning capabilities (Talib et al. 2010; Maurer et al. 2011). Although there is a growing number of ISA initiatives targeting the general public to provide them with the appropriate knowledge to be aware of such threats and be able to make informed security decisions when required, but the awareness of their existence between users is relatively low (Furnell and Moore 2014). Even though, the information presented is general, does not include proper user guidance and fails to follow up.

One of the goals of ISA is to increase users' knowledge and change their behavior accordingly, hence, human security behavior is vital for ensuring an efficient information security environment that cannot depend on technology only. Actually, there are situations of an aware user who knows how to protect himself but, simply, chooses not to. To understand and assess these behaviors, a number of security related theories were used such as The Theory of Reasoned Action (TRA) or the extended Theory of Planned Behavior (TPB) (Khan et al. 2011), General Deterrence Theory (GDT) (Lebek et al. 2013), Protection Motivation Theory (PMT) (Komatsu et al. 2013; Shillair et al. 2015) and Technology Acceptance Model (TAM) (Shropshire et al. 2015).

As the need for ISA among users have been established, the goal is not only limited to having a user who is aware of information security risks. Actually, it is to redefine what is meant by an aware user and go beyond simply giving knowledge, to guiding his behavior to become a security minded user that is able to make an informed decision in detecting and removing information security threats when required. Therefore, a number of research questions and sub questions, in the context of ISA for HU, could be asked as follows:

Q1: How to best define ISA for HU?

Q2: How does ISA relate to information security education and training?

Q3: Is there a difference between ISA of HU and none-home users (NHU)?

Q3.1: What is the relationship between knowledge and practice gained at workplace and home environment?

Q4: Do demographics and cultural factors in different countries have an influence on ISA?

Q5: What is currently done to raise ISA of HU?

Q6: How HU behave online?

Q6.1: What are the factors that influence these behaviors?

Q7: How to motivate HU to protect themselves?

Q7.1: How to best communicate risk to them?

Q8: What are users' preferences of ISA delivery methods?

This chapter is structured as follows: the research methodology is described in the next section followed by some definitions of ISA, education and training. A global study of ISA levels is discussed in section 4. End-user classification, ISA for Home users and how to communicate risks are explained in sections 5, 6 and 7 respectively. A discussion is presented in section 8, and finally a conclusion in section 9.

3.2 Methodology

Since people are always referred to in the security literature as the weakest link, the role of using ISA in reducing information security risks is getting increased attention over the last few years. The aim of this chapter is to provide an up-to-date overview of ISA among members of the general public by answering the above mentioned research questions. To accomplish that, a systematic literature review was conducted where relevant literature was sought in four academic digital databases, IEEExplore, ScienceDirect, ACM and Google Scholar. A list of search terms was used to conduct the search including: ' information security', 'information security awareness' and 'information security behavior'. As the aim of this chapter to present an up-to-date overview of the selected topics and answer the research questions, deemed that papers from 2010 will be suitable, thus, publications before the year 2010 were not considered. Further to that, relevant literature in the field of ISA and behavior was selected using an inclusion/exclusion criteria. Only conferences and journals related to the selected topics were included and non-academic articles were excluded. This resulted in an initial list of 1884 articles. Then, articles that do not mainly deal with ISA and user behavior were excluded. This was done by reading the articles' titles, abstracts, keywords and a quick scan of the full text.

Additionally, reference checking for relevant articles and citations was done. Finally, 5 technical and statistical reports, 8 websites and 2 books were added as relevant. This resulted in a final list of 74 articles as shown in Figure 3.1.

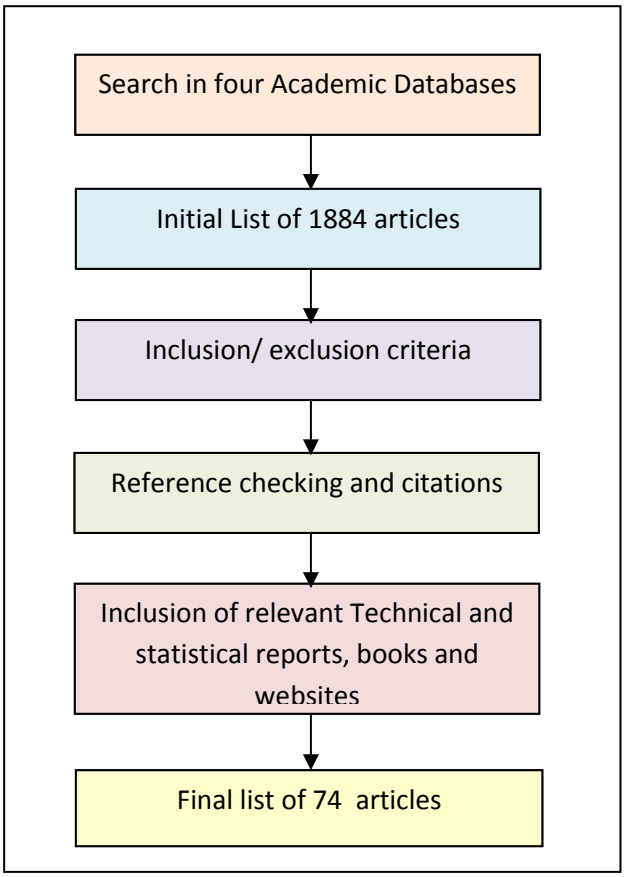

Figure 3.1: Review Research Methodology

3.3 Information Security Education, Training and Awareness (SETA)

The intensive sharing of information among users through emails, social networks along with lack of ISA to protect themselves make them an easy target for attackers. Users both pose and face risks and their devices may be used with or without their knowledge as attack vectors such as botnets (Al Sabbagh et al. 2012). This implies that users require SETA, to increase their knowledge, self-confidence and accept personal responsibility to protect themselves and, eventually, others. In order to help understand when to train, educate and/or aware users, the differences between these concepts should be understood. However, the definitions of these non-technical aspects may not be clear and complete as one would think and sometimes used interchangeably in the literature (Hansch and

Benenson 2014). For example, Amankwa et al. (2014) performed a conceptual analysis of information security literature and found that ISA, education and training are different concepts with regards to their focus, purpose and delivery method as in Table 3.1.

	Information Security Education (ISE)	Information Security Training (IST)	Information Security Awareness (ISA)
Focus	Insight and understanding	Information security skills and information security knowledge	Attention directing and reminders
Purpose	Equip employees with the skills and competencies needed to ensure CIA of Organization information	Equip employees with information security skills and information security knowledge specific to their roles and responsibilities	Ensure that every employee realize their role and responsibility towards protecting the Organization's information
Method of delivery	Theoretical instructional methods in the form of seminars, classroom discussions and research	Practical instructional methods in the form of seminars and workshops	Print and electronic media such as videos, flyers and posters

Table 3.1: Definitions of SETA (Amankawa et al. 2014)

ENISA (2010) defines ISA as " *Awareness tries to change the behavior and patterns in how targeted audience (e.g. employees, general public, etc.) use technology and the Internet and it is a distinct element from training. It consists of a set of activities which turn users into organizations' first line of defense. This is why the awareness activities occur on an ongoing basis, using a variety of delivery methods and are less formal and shorter than training*". NIST SP 800-16 (1998) define ISA as " *Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly*". Whereas Stewart and Lacey (2012) define ISA as " *The broadcast of facts to an audience in the hope that their behavior improves".*

Information security training is an important concept in information security. A number of definitions of information security training are found in the literature. Wilson and Hash (2003) define it as " *Training seeks to teach skills that allow a person to perform a specific function".* According to NIST SP 800-16 (1998) "*Training strives to produce relevant and needed security skills and competencies".* While ENISA (2010) define and differentiate between training and awareness as

"*Training seeks to teach skills which allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues".*

Information security education may seem closely related to training. It is everything done to help users perform their roles successfully and appreciate the need for information security (Sedinic et al. 2014). NIST SP 800-16 (1998) points out to education as " *integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge*". Wilson and Hash (2003) suggest that information security education "*focus on developing people's ability and vision to perform complex multi-disciplinary activities and the skills needed to further the information security profession and to keep pace with threats and technology changes*".

However, these definitions mainly focus on the broadcast of facts which is what is suggested by IT experts. This may make these definitions limited. This view may have stemmed from the fact that IT experts assume that users possess far too much knowledge than they actually do and build their expectations on this (Furnell and Clarke 2012). Additionally, focus is on technical aspects and performed tasks where factors such as culture and learning styles are overlooked. Hence, to avoid overwhelming the user with information already known to them, there has to be a focus on what they *do not know* and *need to know*. As a result, ISA could be defined as the attempts to *raise user's information security knowledge* according to their needs to be able to properly detect and remove information security threats and direct the change of their behavior to correctly implement security measures. Whereas, training could be defined as the attempts to develop user's *skills and ability* to detect and remove information security threats and direct the change of their behavior to correctly implement security measures. Finally, education can be defined as developing user's ability to *understand and appreciate the need* for various activities d to detect and remove information security threats and direct the change of their behavior to correctly implement security measures.

Thus, ISA can be described as an ongoing process to reflect the evolving threat landscape and can be perceived as the '*What to*' learn component. Whereas training and education could be perceived as the *'How to'* and *'Why to'* learn components respectively. Although they share a common goal which

is to change user's behavior, but education is more generic and uses theoretical delivery methods whereas training is more specific and uses practical delivery methods.

As these are well-established disciplines in organizational context, it is a challenge to include a more general population, HU, due to their lack of time, motivation and varying levels of prior knowledge and expertise. Additionally, it is hard to determine if they are well equipped to go online (Furnell et al. 2008). This implies a joint effort approach to create a security minded user that is aware of the information security threats, why to protect form them and , and finally, how to make a proper informed decision in reacting to them. For example, in the case of a non-updated Anti-Virus software, instead of just prompting the user that his software is out of date and needs to be updated, a more informed and understood approach could be used (Furnell and Moore 2014). The user could be informed, roughly, as follows:

Your Computer is AT RISK due to out-of-date Anti-Virus software	(*raising Knowledge through ISA*)
11367 new viruses cannot be detected by your Anti-Virus software	(*Appreciate the need for an update through education*)
To update your Anti-Virus software click the ….	(*How to do it through training*)

An attempt has been made by (Hansch and Benenson 2014) to reach a common definition of ISA. They analyzed the literature to find what ISA means implicitly and explicitly to researchers. They found that ISA could be defined as perception or knowledge where they need to be aware of threats, as protection or attitude and a change in how they think and belief of them and what they are, and finally, as behavior or change in behavior. Accordingly, knowledge of information security concepts enable users to realize the relationship between information security elements and , therefore, help ensure that the given knowledge is used or implemented. This may enable users to understand the necessity of applying this knowledge and reason in choosing the best way to applying it. So, users need to be aware of a threat and then realize that this threat or risk needs to be dealt with (Harbach et

al. 2014). Therefore, a mapping of ISA, training and education to Knowledge, attitude and behavior (KAB) could be as shown in Figure 3.2. However, to maximize behavioral change, SETA has to be performed together.

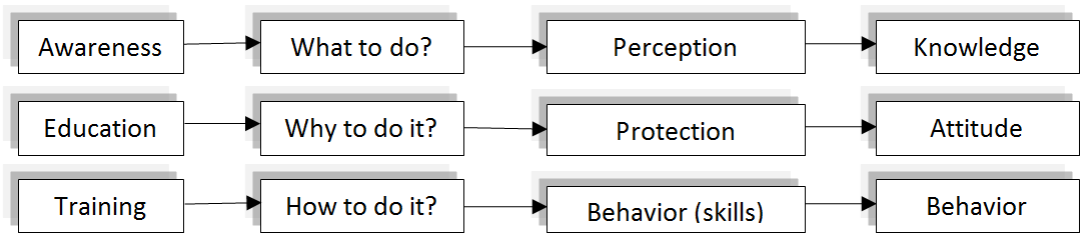

Figure 3.2: Suggested Mapping of SETA to KAB

3.4 ISA in Countries

Although the importance of the need for ISA and the devastating risks of information security threats are generally well understood, it has been found in the literature that there is a digital divide within countries. In a study by Kaspersky Lab, 44.51% of web attacks in 2017 were carried out from malicious web resources located in the United States and Germany (Kaspersky 2017). A statistics about the top 10 countries where users face the greatest risk of online infection is as in Table 3.2. According to Kaspersky Labs, these statistics show unique users whose computers have been targeted by Malware-class web attacks as a percentage of all unique users of certain Kaspersky Lab products in the country (Kaspersky 2016; Kasperskay 2017).

2016			2017		
No.	Country	% of unique users	No.	Country	% of unique users
1	Russia	42.15	1	Algeria	44.06
2	Kazakhstan	41.22	2	Belarus	38.39
3	Italy	39.92	3	Russia	36.91
4	Ukraine	39.00	4	Kazakhstan	36.57
5	Brazil	38.83	5	Tunisia	36.51
6	Azerbaijan	38.81	6	Vietnam	35.01
7	Spain	38.21	7	Azerbaijan	34.70
8	Belarus	38.04	8	Qatar	34.20
9	Algeria	37.11	9	Portugal	33.01
10	Vietnam	36.77	10	Greece	32.80

Table 3.2: Top 10 countries of online infection

One might ask if there is a relationship between socio-demographic and country-based differences and the level of ISA of users? To answer this question, a review of several country-specific studies have been undertaken and presented in Table 3.3.

From the these studies, it is apparent that there is a challenging general low level of ISA among users whether in the contexts of generally using the Internet, in smartphones or in social networks. Further to that, it is evident that there is a relationship between some socio-demographic factors and the level of ISA among users that makes them vulnerable to information security threats. The key socio-demographic factors that were found to have an influence on ISA are as follows:

1) **Language, i.e. Mother Tongue**: This factor has an effect on users comprehension of technical terms they may face when they are online. As a result, it is recommended to use more than one language when designing ISA materials. However, it is not necessary to translate the term itself, but explain the concept and related risks in the appropriate language.

2) **Age**: In most of the ISA literature, the age distribution that showed a high percentage of user group with ages less than 30 years old, mostly college students. This may be considered normal as young people are more interested in voluntarily responding to surveys related to ICT usage as they are more familiar with the technology than other groups. Thus, they are not good users of it (Furnell and Moore 2014). Another reason is because this age could be linked to risky behavior such as their preference of pirated (jail broken) smartphone applications where users of this age group tend to engage in risky behaviors may be as part of their learning journey (Ophoff and Robinson 2014).

3) **Percentage of daily online activity**: As risks materialize with increased online exposure (Rughiniş and Rughiniş 2014), it has been found that in countries where online activity is widely spread, users engage in more diverse and intense use than daily users of Internet in countries with less Internet popularity.

4) **IT expertise**: It has been found that the higher the level of IT expertise or security education the more they are cautious in their online behavior as they are more aware of

information security threats and tend to adopt security controls to protect themselves. Moreover, the more a community is high-tech, the more they are concerned about privacy and security (Harbach et al. 2014)

5) **Gender**: Females were found to be more vulnerable to information security threats such as phishing more than males. This may be due to several reasons which accounts for this susceptibility and less security control adoption. Reasons such as they arguably have less IT expertise and security knowledge than males and the differences in the way males and females use the Internet or make trust decisions.

6) **Culture**: It was evident that cultural factors play a role in the level of ISA among users especially in multi-cultural and/or developing countries such Saudi Arabia and South Africa. This implies that these country-specific cultural differences should be considered when designing materials to increase the level of ISA among users especially that there are common known risks and culture-specific risks (Harbach et al. 2014).

Researcher	Sample Demographics	Findings	Comments
Aloul (2010)	- United Arab Emirates - Sample population of students and staff in American University in Sharjah.	- The controlled phishing experiment demonstrated low levels of ISA regarding phishing attacks - The wireless network security assessment revealed a lack of wireless network security awareness with weak encryption mechanisms or no encryption at all.	- Study was limited to one University only. - Results generalized carefully as it may not be representative of a larger population.
Hasan and Hussin (2010)	- Malaysia - Sample population of 119 college students who responded to a closed-end survey	- Most of Social Networks (SN) users are not fully aware of what information to be released on SN and what are the consequences if such sensitive and personal information is revealed such as their physical location, when gone away for a vacation or email password.	- Findings are Consistent with the literature that no high appreciation of security and privacy in this age group (college students). - More enhanced results if a more comprehensive sample was used such as high school students and working adults
Sheng et al. (2010)	- United States of America - Sample population of the general public	- Gender and age can be used to predict susceptibility to phishing. - Users with age group 18-25 and Females are more vulnerable to phishing attacks than males	- Results could be more generalized than those of (Aloul, 2010) as they reflect direct relationship between demographics and phishing susceptibility - Studied the effectiveness of some anti-phishing education delivery methods (an online game and a comic)
Kruger et al. (2011)	- South Africa - Sample population of 180 students in two universities that answered an online two-section questionnaire of a vocabulary knowledge test and scenario-type questions.	- Cultural factors such as area where you grew up and language have an impact on ISA whereas gender, field of study and how long the participant had used a computer do not have a significant effect on ISA - The need for ISA programs with a focus on social engineering	- Low response rate - The use of a knowledge test is a major advantage of this study as it is an acceptable way for assessing user's level of comprehension and security knowledge background
Alarifi et al. (2012)	- Kingdom of Saudi Arabia - Sample of 462 online survey respondents	- Due to Saudi tribal and patriarchal culture, and high levels of censorship low level of ISA among the Saudi general public was found in general especially in password practices, DDos attacks, phishing, how to report a security incident and use of Anti-Spam and Anti-Spyware mechanisms. - High ISA levels of viruses and Anti-Virus software use. - Use of protection is lower than the awareness of Information security threats.	- Used an Arabic online survey to ensure respondents comprehension of questions. This may be a drawback because English is the dominant language of the Internet - No indication of demographics in the survey such as age, gender and level of education as these, due to Saudi culture, may add more depth to results

Bostan and Akman (2013)	- Turkey - Sample of 433 survey participants of the general public	The existence of important relationships between frequency of use, reason for ICT usage and email security and several factors related to socio-demographics such as gender, age and education.	- Sample did not represent different groups of the society such as IT experts. - More interesting to include other socio-demographic factors such as income and effect of culture on ICT usage
Ophoff and Robinson (2014)	- South Africa - Sample population of 619 respondents to an online survey to assess their level of smartphone ISA	- In general, low level of smartphone ISA especially in highly trusting application repositories, pay little attention to security and privacy measures and low level of security control adoption - Users with IT knowledge have "Deterministic views" on testing smartphone applications which affects their trust in application repositories - No evidence that cultural factors or language have a significant effect on ISA	- Contradicts findings of (Kruger et al.2011) that language has an effect on ISA. This context of study, smartphones, and its relatively high purchasing cost may have limited the sample to users of higher economic means with a good command of the English language. This resulted in biased results, where 70% of respondents English language was their mother tongue. This does not reflect the multicultural aspect of South Africa.
Rughiniş and Rughiniş (2014)	- European Union (EU) - Survey, Eurobarometer 77.2/2012 dataset	- Countries in the EU with higher percentage of daily Internet users foster cyber security cultures. - High ecological correlation among daily Internet users between country level frequency of Internet use and occurrence of security incidents where security behavior was found to be high - Correlation is weaker between Internet use and cybercrime exposure. - Relatively low social stratification of password hygiene and cybercrime exposure along age and educational achievement	- More detailed investigation of security and online activity may have resulted in deeper analysis of users' online behavior.
Filippidis et al. (2018)	- Greece - Sample population of University students	- Although students were aware of information security issues, they have limited knowledge in the adoption of security tools and techniques. - Study program and educational level have a positive impact on the level of information security awareness and computer ethics - No evidence that gender has an impact/role on the level of information security awareness and computer ethics	- Findings are consistent with most of literature on the role of gender, study program and educational level on ISA - The study is somehow limited in terms that the sample population was from a single university. - A good advantage of this study is that it highlighted the importance of adopting open/free software in education especially with the found high rate of phishing, social engineering and spam among students against each other.

Table 3.3: A review of ISA in countries

3.5 End-users' Classification

One of the ways to better understand Internet users and help create more effective ways in communicating information security risks to them is by classifying them (Blythe et al. 2011; Kruger et al. 2011; Martin and Rice 2011; Stewart and Lacey 2012; Shillair et al. 2015). However, different classifications of users could be obtained depending on the used classification criteria.

Rughiniş and Rughiniş (2014) classified Internet users theoretically based on their behavior as security actors into three models. They claim that user's behavior could be interpreted, for analytical purposes only and not empirical, with regards to each of the specified theoretical perspectives. However, each of these models include both risk-seeking and risk-averse behaviors. An explanation of each model is found in Table 3.4.

	Cognitively lazy users	Economically rational users	Social users
Portrayal focus	Technical naïveté, due to multiple objectives	Economic rationality in the context of one's own activity	Self-presentation concerns; trustful actors, in pursuit of concerted activities
Users' risk awareness	Awareness is dim, risks are underestimated	Awareness is adequate, reflecting estimated personal risks	Relevant risks are socially defined, through communication that gives meaning to personal experiences
Rationality	Bounded, based on heuristics	Economical, based on cost-benefit analysis	Rationality appears as a byproduct of activities of justification (accounting), using socially constructed vocabularies
Main springs of action	Satisficing on goals Minimizing effort	Optimizing the pursuit of preferences	Achieving legitimate goals and maintaining desired identities in the local social order
Reasons for low compliance	Low understanding of risks and low technical expertise	Average end-user losses from cybercrime are perceived to be low; Security costs are high; Future costs and benefits are discounted	Security practices are: - Obstacles for smooth social organization - Associated with de-valued identities

Table 3.4: Theoretical model of end-users as security actors (Rughinis and Rughinis 2014)

It is apparent that differences in the above mentioned users' security behavior depend on user's experience of loss, reasons behind their taken security behavior and on the resources they can access to obtain technical expertise to devise an economical solution. Later, they used K-means cluster analysis to classify users based on survey data obtained from the Eurobarometer 77.2/2012 dataset. The resulting classification is as in Table 3.5 with a mapping to their proposed theoretical models.

Theoretical Model	User Type	Behavioral Indicators		
		Frequency of Internet Use	Experience of Cyber Crime	Use of Security Measures
Social user	Explorer	High	High	High
	Reactive	Average	High	High
Economically rational	Prudent	Average	Low	Low
Cognitively lazy	Lucky	High	Low	Low
	Occasional	Low	Very low	Very low

Table 3.5: User Types

This survey based classification of users is a valuable resource for the design of public security policies, public interventions and a meaningful interpretation of users' actions and in linking them to social contexts. However, such classification could have been improved if additional measures were included. Examples of such measures are security knowledge, estimations of cybercrime personal loss in terms of reputation, money or time and whether these losses resulted from work or from personal online activities. Furthermore, more detailed investigation of security and online activity may have resulted in deeper analysis of users' online behavior.

Another criteria for classifying users is presented by Kritzinger and von Solms (2010) as they classified users according to the source used for Internet access and whether it is through a personal device or through devices within the work environments. Accordingly, this resulted in the following classification:

- **Home Users (HU)**: These are users who access the Internet through their home environments using their own personal computers and are responsible to secure these computers. They are not essentially forced to obtain information security knowledge in any form.
- **Non Home Users (NHU):** These are users who access the Internet through their work environments such as Governments, Universities and Private sector enterprises. This kind of users sit under the administrative umbrella of their organization. They gain Information security knowledge through their working environments in the form of

ISA, training and education which are governed by procedures, policies, guidelines and best practices. These are enforced and implemented under a watchful eye of their organizations to ensure compliance with such regulations.

Furnell and Thomson (2009) classified NHU according to their security behavior in terms of compliance and commitment to security as shown in Table 3.6.

Compliance	Culture	The ideal state, in which security is implicitly part of the user's natural behaviour.
	Commitment	Security is not a natural part of behaviour, but if provided with appropriate guidance/leadership then users accept the need for it and make an associated effort.
	Obedience	Users may not buy into the principles, but can be made to comply via appropriate authority (i.e. implying a greater level of enforcement than simply providing guidance).
	Awareness	Users are aware of their role in information security, but are not necessarily fully complying with the associated practices or behaviour as yet.
Non-compliance	Ignorance	Users remain unaware of security issues and so may introduce inadvertent adverse effects.
	Apathy	Users are aware of their role in protecting information assets, but are not motivated to adhere to good information security practices.
	Resistance	Users passively work against security, opposing those practices they do not agree with
	Disobedience	Users actively work against security, with insider abusers intentionally breaking the rules and circumventing controls.

Table 3.6: Levels of security compliance based on security behavior (Furnell and Thomson 2009)

Whereas one of the goals of ISA of HU is to ensure that they comply to guidelines and best practices and to create a sense of responsibility in which users promote security oriented behavior without the need for a watchful eye, then this classification could be generalized to include HU. However, describing users' behavior using words like ignorant or lazy may by a narrow and limited view as some limitations may be placed on them are ignored in terms of resources, time and learning capabilities.

Another user classification criteria is used by Furnell et al. (2007) as they classified users according to their security knowledge in terms of how long they have been using the Internet to:

- **Novice users:** These are users who have been using the Internet for a average of 4 years
- **Intermediate users**: These are users who have been using the Internet for an average of 8 years

- **Advanced users**: These are users who have been using the Internet for an average of 10 years

However, it is worth noting that this period of using the Internet does not reflect the user's ability to protect himself nor his ISA level. Shillair et al. (2015) Classified users according to their prior knowledge of online protection to Naïve and experienced users. As no criteria was specified for measuring this knowledge, thus, it is important to ensure how knowledgeable they are especially with the evolving online threats.

From an analysis of user's classification, Figure 3.3 represents a taxonomy of end users. Understanding how to classify users is a key factor to better ISA. Nevertheless, none is right or wrong but it is an attempt to better understand the users.

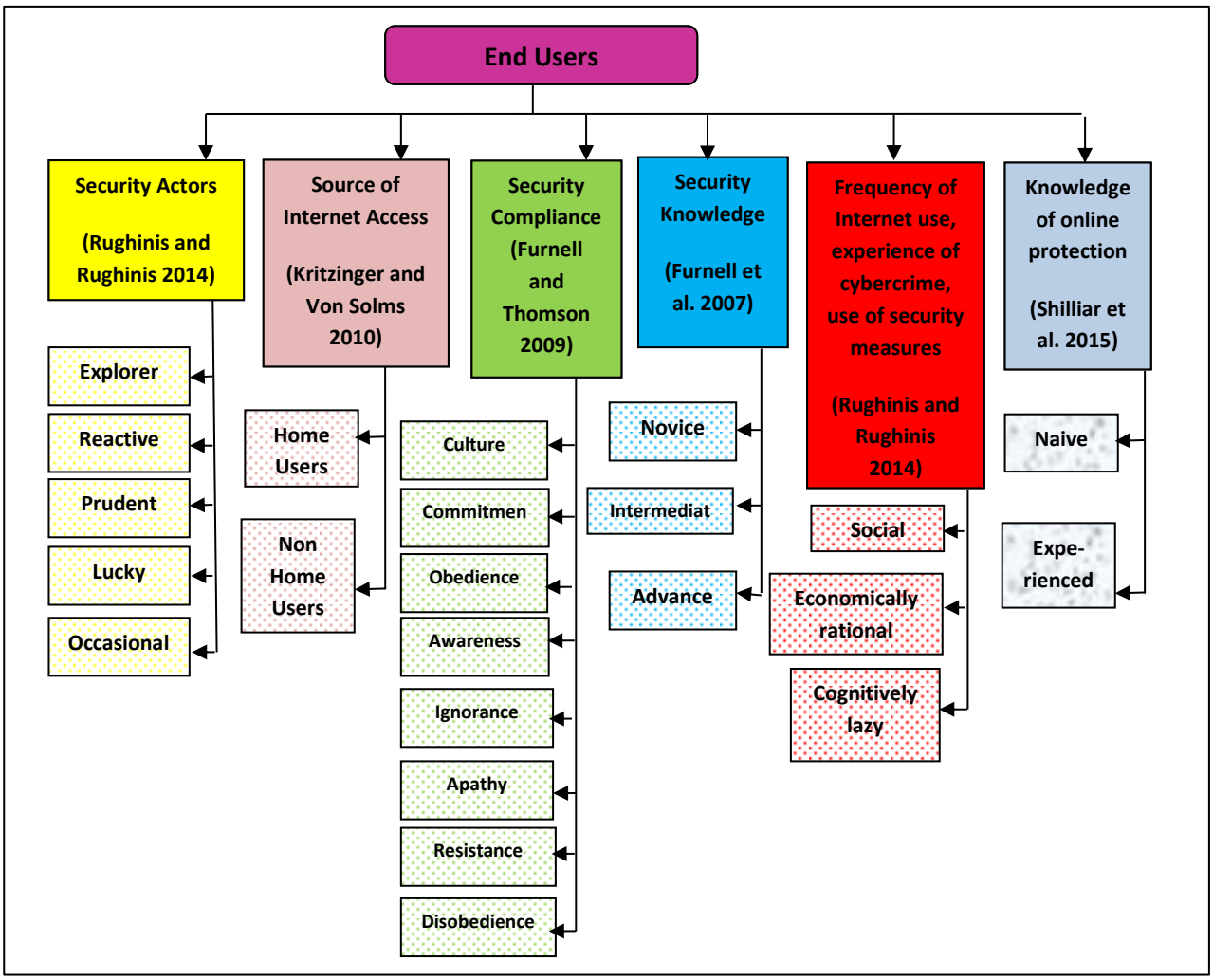

Figure 3.3: End Users Taxonomy

As one of the objectives of this research is to investigate and develop a novel approach to ISRA and communication for the general public, additional aspects could be included together with the already used classifications, users could be classified, as in Figure 3.4, according to:

- Online activity such as low and high.
- User's age such as children, teen agers and seniors.
- Type of used technology (infrastructure or platform) such as smart phones and WiFi.

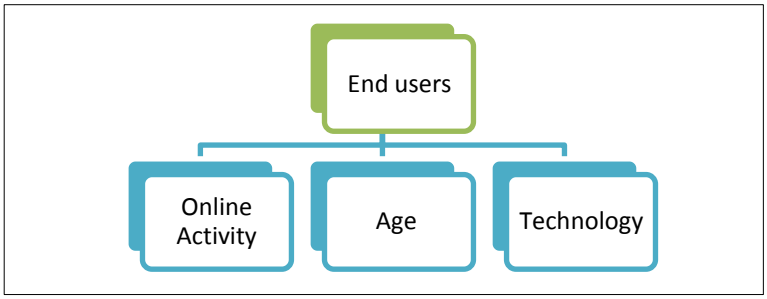

Figure 3.4: End users classification

3.6 ISA for Home Users (HU)

Given that HU are mostly untrained in information security protection, they are likely to be vulnerable to information security attacks (Furnell and Vasileiou 2017) . One of the reasons behind HU arguably lack of ISA is that ISA is not enforced by a third party to ensure that HU ISA is up-to date-or at least they use the Internet securely (Kritzinger and von Solms 2010; Talib et al. 2010; Kritzinger and Von Solms 2013).

To understand the difficulties that HU face and their attitudes towards online security, Furnell et al. (2008) conducted interviews with an indicative sample of 20 novice users. Their findings suggest that their online security practices are due to weakly formed technical knowledge or difficulties posed by security tools such as being annoyed by too many warnings and pop ups that results in them disabling the features that are the causes of these disturbing messages. On the basis of their findings, they suggest that to overcome this ill-informed behavior, security decision making should be removed from the user by either removing the user's choice or reliance on him in matters related to security protection. Even though the used data collection method is considered as an effective method of allowing users to discuss their experiences about their online behavior, but these views may be incomplete and biased as

participants may feel obligated to pretend a more cautious behavior just to not seem careless or ashamed . However, more depth could have been given to these findings if the reasons behind why users where found to be less motivated to protect themselves were further investigated and analyzed. This may have resulted in an in-depth understanding about their security behavior.

A similar study was conducted by Albrechtsen (2007) but in an organizational context to investigate users' experience of information security and their role in the work of information security. The author conducted qualitative interviews with employees of a Norwegian bank and an IT-company. Later, a summary of these interviews where sent by email to participants for acceptance and control. The interviews revealed that ISA campaigns had little effect on employees security behavior and a preference for group discussions as an effective method for influencing their behavior. Although this is an important study that highlights the information security concerns of employees in organizations and their understanding of information security processes, but users' views may be biased as a result of face-to-face interviews for the reasons stated earlier. Thus, the results would have been more indicative and less-biased if participants were presented by a list of security actions for example.

The findings of Harbach et al.(2014) give stronger indications about users' awareness of risks while using the Internet as they used an online survey to reach users' in their familiar settings and a population in two continents to explore the differences in risk awareness between them. This is evident as they found some cultural-specific risks. A good aspect of the used data collection method is that the authors used a two section questionnaire. In the first section, participants were given five scenarios and asked them to list which risks they were aware of. The second section was a precompiled list of 22 common risks in which participants were asked to identify the ones they were aware of and how relevant they are to them. Later, to minimize bias in results, the authors compared between participants' answers to both sections. Their findings suggest that end-user security could be improved by addressing risks which are

salient to them and already aware of or by changing risk perception through education and risk communication.

Martin and Rice (2011) collected the views of 66 computer users and organization employees to identify their major concerns and provide advice accordingly. Their findings suggest that the treatment and handling of users' personal information such as what personal information to be revealed in social networks is a key element in addressing cybercrime concerns. However, despite the small number of individuals input, most input came from large to medium sized organizations in both public and private sectors. Thus, one might think that these results are biased or represent employees views but this is not the case as it is consistent with members of the general public concerns found in Furnell et al. (2008) and Harbach et al. (2014).

These studies were selected and reviewed to have a comparison between information security concerns of both employees and users from the general public. It was found that there is a difference between them as employees concerns were mainly focused about their role as employees in the information security process of their organizations. Whereas users from the general public concerns were about information security risks, cybercrime and how to well protect themselves from them. A summary of these studies is in Table 3.7.

	Albrechtsen (2007)	**Furnell *et al*.(2008)**	**Martin and Rice (2011)**	**Harbach *et al*.(2014)**
Sample population	Employees of an IT company and a bank (private sector)	Novice users	Employees of Government, Non-Government, public and private companies, and individuals	University Students and United States based workers
Data collection method	Face to face interviews	Face to face interviews	Parliament of Australia web pages	Online questionnaire
Country	Norway	United Kingdom (UK)	Australia	Germany and United states
Analysis	Not specified	Not specified	Concept analysis and mapping techniques	ANOVA and p-value test

	Albrechtsen (2007)	Furnell *et al.*(2008)	Martin and Rice (2011)	Harbach *et al.*(2014)
Findings	Concerns for their role in Information security in general: - Aware of their Information security responsibility, but do not perform many Information security actions. - Priority conflict between functionality and Information security workload - User-involving approach is the best way to influence behavior and ISA	Concerns for protection in general: - Aware of existence of information security threats but less aware of appropriate safeguards - Aware of their responsibility of protecting themselves but less concerned about impacts - Lack of technical knowledge and usability problems are obstacles in achieving protection	Concerns for cybercrime in general: - Concerns for Identity theft, financial fraud, spam, phishing and botnet attacks - Frequency of Information security incidents and malware threats - Need ISA and education - Role of Laws in preventing cyber crimes - Installation and use of security software - Cyber bullying	Concerns for risks and consequences in general: - Privacy (loss of privacy, theft of private information) - Account abuse - Malware and hackers (infection with malware, phishing, spam) - Financial risks (theft of credit card details)

Table 3.7: A Comparison between End-users' Information Security Concerns

However, as some users could be part of both environments, one could ask if ISA knowledge and practices gained at the workplace could be transferred to the home environment and *actually* practiced? This was explored by Talib et al.(2010) as an online survey was used as a data collection tool that attracted more than 300 respondents. Their findings suggest that respondents who took security training were found to be more aware of a variety of security issues than those who did not. Moreover, they appeared to be motivated to take a form of security education given some flexibility in what to learn, when and how. Surprisingly, 95% of respondents who had training stated that what they learnt in the workplace is key to what they actually practice at home. Although their findings addressed the need for ISA strategies that provides information security training and education to users regardless of their environment, but such results should be generalized into a wider population cautiously. This is because respondents had a good level of ISA and practices and may not represent the wider population as it is expected they have lower levels of ISA and in IT in general.

3.6.1 Solutions to Protect Home Users

Since the lack of awareness of online risks is one of the reasons behind HU becoming vulnerable to information security threats and an attractive target for attackers, Kritzinger and von Solms (2010) proposed an E-Awareness Model (E-AM) to improve ISA among HU by presenting some information security content and enforcing the users to understand this content. This proposed model is composed of two components:

- E-Awareness portal or a "what a user should know" component.
- The enforcement component or the "how the content absorption can be enforced" component.

This proposed model, as in Figure 3.5, is a theoretical model with no implementation, so it has not been tested or evaluated yet. Further to that, the viability of this enforcement approach is questionable especially in terms of user's acceptance. However, authors claim that a prototype is currently under implementation and will be tested in a school environment.

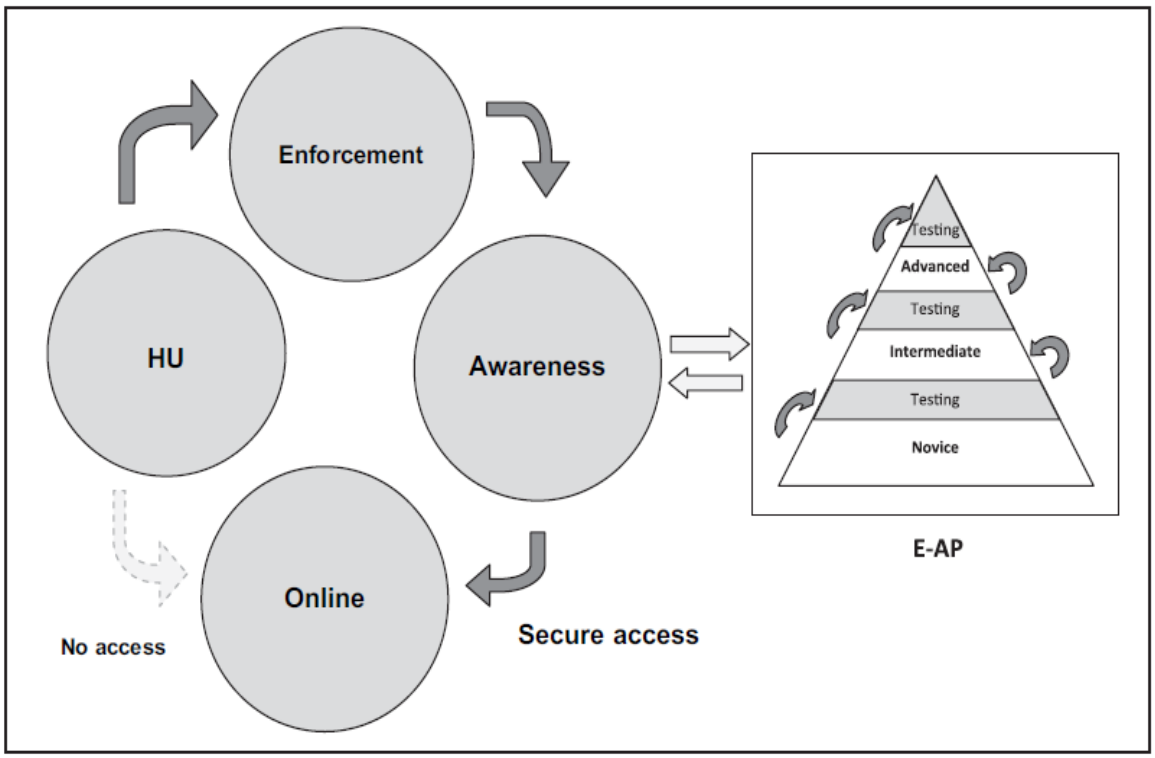

Figure 3.5: The E-AM model (Kritzinger and Von Solms 2010)

A next extended version of this proposed model is presented by Kritzinger and Von Solms (2013) where most of the security responsibility such as patching and Anti-Virus protection are moved away from the HU and hosted by the regulating body. In this sense, they proposed a migration approach of three steps to help users become more secure by increasing the security responsibility of ISPs and decreasing it for HU. The approach is as depicted in Figure 3.6.

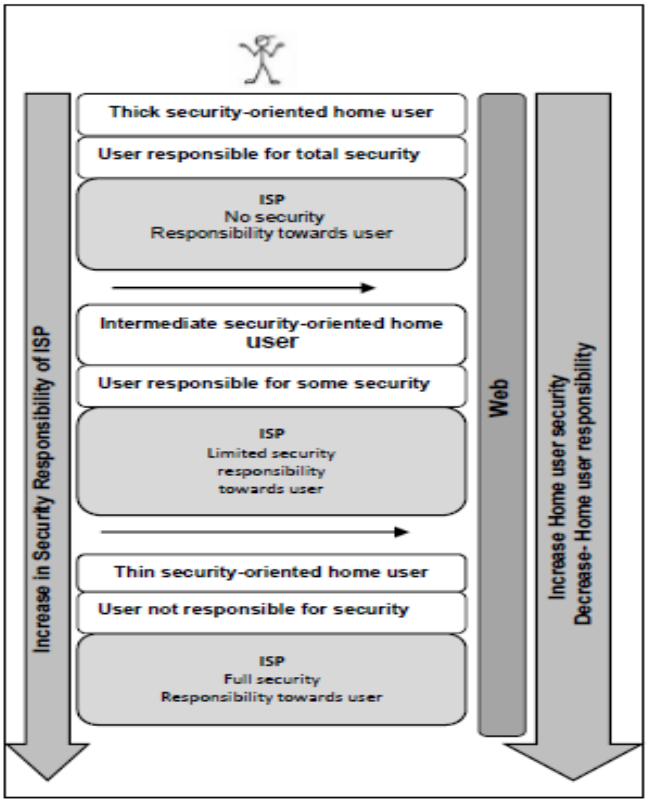

Figure 3.6: The Three steps Framework (Kritzinger and Von Solms 2013)

Assuming that ISPs will accept this expanded type of this responsibility, this technically oriented approach is a way of enforcing security protection on the user that is consistent with the security literature that suggests to remove the security responsibility away from the user (Furnell et al. 2008; Furnell and Clarke 2012; Rao and Pati 2012). However, an extra effort will be placed on the ISP in terms of software, processing and management. Furthermore, this effort has to be paid for which may place a cost overhead on the HU. This may result in him simply rejecting this approach especially if he does not appreciate the need for it. Nevertheless, ISPs are not the guarding angels of users and may not have the legal or ethical position to make such

decisions on behalf of the user. Additionally, some users may perceive this ISP intervention as a violation to their privacy and may hold ISPs responsible if something bad happens. This implies that a trust relation has to be established between HU and ISP beforehand.

Nevertheless, ISPs can play an important role in providing users with awareness on internet security issues and assisting them to protect themselves from online threats such as with using anti-spam and anti-virus software (Adelola et al 2015). Not limited to ISPs, but outsourcing security in general as in security-as-a-service (SECaaS) that includes security software that is delivered on the cloud and in-house security management offered by a third party (Chaisiri et al. 2015). In this manner, internet-connected applications can use security services such as spam filtering and anti-malware to protect applications and data against various online threats. Instead of installing such security tools and managing them by the user, these services are utilized using a web browser which makes it direct and affordable (Wenge et al. 2014). Some examples of the offerings of SECaaS as outlined by the Cloud Security Alliance (Cloud Security Alliance 2018) include data loss prevention, encryption, email security, web security and Identity Access Management (IAM).

As security is a significant problem in many online services, many SECaaS solutions are offered by product vendors such as Cisco, Symantec, McAfee and Verisign or as methodologies in the literature such as Hussain and Abdulsalam (2011), Hasan and Moftah (2013), Sharma et al. (2016), Kim et al. (2017), Chen et al. (2018) and Chawla and Thamilarasu (2018). Unfortunately, most of these tools and methodologies are designed for organizations and lacking for home users.

However, SECaaS is used in many aspects such as in storing authentication biometrics in the cloud (Yousif 2016). In a study by Erdim and Sandikkaya (2019), a cloud-based architecture is proposed for a one-time-password as a service to help users change their conventional authentication scheme of username/password to a more secured scheme. Since it is hard to prevent problems arising from users insecure behaviors, this architecture does not solve conventional username/password usage flaws such as vulnerability against guessing

attacks or memorization problem. Conversely, as a result of such problems, a second factor to conventional authentication is added.

Some internet services request users to provide sensitive information such as ID and credit card numbers. However, the way in such sensitive information is used is determined by the service provider only and users have no other choice but to allow such usage. Takahashi et al. (2011) proposed a framework that allows users to choose the way in which their information is protected through the use of a policy that is offered as a SECaaS. This is achieved by incorporating the information protection type in a program, according to the policy, in which the service provider will use their sensitive information through this program. However, this is a theoretical framework that has not been tested in reality, hence its validity and applicability remains uncertain.

Users are delegating service providers who run IAM management systems to manage their log in credentials among other sensitive information. However, only 23% of the population sample of the survey conducted by Abdulwahid et al. (2015) were willing to pass this responsibility to a third party. This highlights a low preparedness rate and the need to have users understand such mechanism. Further to that, as the security environment is not controlled in an in-house manner, the concerns over SECaaS have the right to exist. This could be because SECaaS user-provider relationships are distant as users access the offered security services remotely which may reduce the personal contact level and, as a result, exacerbate security threats. Hence, security in the context of SECaaS is related to trust (Goode et al. 2015). Additionally, users' perceptions of SECaaS providers robustness can be affected. This is due to them serving many users over the same network infrastructure and at the same time having access to each user's data (Kim et al. 2011). Security mechanisms are complex and users are only aware of those mechanisms that affect their service requirements. Although other security mechanisms offered by SECaaS providers are important, but their functionality is invisible to the users. As security relates to their own operations depending on the threats they face, this

raises users' concerns over the perceived value of such mechanisms especially that security is subjectively perceived by the user (Goode et al. 2015).

A variety of resources are at the disposal of users to improve their awareness of information security threats. Many of the major Anti-Virus providers, Governments and Operating System vendors have some dedicated resources to increase users' knowledge about information security. An extensive online resource is offered by Microsoft (Microsoft Internet Safety and Security Center 2015) to teach users about information security and includes lists of advices for users to become secure. Moreover, McAfee (Home.mcaffee.com 2015), the well-known Anti-Virus provider, has an online resource that gives security advice and tips to users on how to protect themselves. Even Governments are starting to recognize their role in satisfying the need for ISA. This is evident with the growing number of Government sponsored initiatives that are targeting the general public. Examples of such initiatives are the StaySafeOnline.org (USA) (Staysafeonline.org 2015), GetSafeOnline.org (UK) (Getsafeonline.org 2015), CyberStreetWise.com (UK) (Cyberstreetwise.com 2015) , The BBC Guide to using the Internet (UK) (BBC WebWise 2015), ENISA's Guide on How To raise ISA (EU) (ENISA 2010) and the guide published by the German Federal Academy of Public Administration (Germany) (Hansch and Benenson 2014) to name a few.

As these maybe considered as good guidance resources to those who realize they need it and look for answers, but they are not easy to find by users as they may lack the skills and knowledge to find them. Unfortunately, this was confirmed by (Furnell and Moore 2014) as they found that awareness of the existence of such resources is relatively low. Even if they are aware of them, they do not know which level of information security knowledge is relevant to them. However, they generally suffer from the following disadvantages:

- Most of the information in these resources are presented in a text based fashion with some occasional video files aimed at providing assistance in informing and educating members of the general public to improve their online safety behavior.

- Most of these resources provide beginner's information with no dynamic user actions, such as examples and exercises, and may not contain regularly updated information.
- They are generally not well structured where users may find it difficult to search and find certain information.
- No proper guidance on the selection and implementation of security controls is provided.

Further to these online resources, there are some Government sponsored activities such as the National Cyber Security Awareness Week by the Australian Government to promote safe computing practices (Martin and Rice 2011), The Get Safe Online Week and Safer Internet Day by the UK Government.

Alotaibi et al. (2017) did an analysis of the efforts made in providing information security education and awareness for HU. Their analysis suggested that regardless of the significant efforts made, a focus upon a "one-size-fits-all" solution was apparent with no consideration of the needs, security priorities, prior knowledge and learning styles of users. This resulted in information overload and users spending lots of time reading web-based content that may have little relevance to them.

3.7 Risk Communication

Improved information security requires effective risk communication to users. This need for effectiveness is critical due to the evolving threat landscape and the need to adapt to new threats and their security countermeasures. Additionally, improved risk communication about information security risks is required to change user's behavior. Typically, risk communication consists of security expert designed messages to inform or educate non-expert users about risks (Asgharpor et al. 2007; Blythe et al. 2011; Blythe and Camp 2012; Stewart and Lacey 2012). Thus, it may be considered as the first step in enabling the users to make informed security decisions. Although these messages are designed by experts who know the risks, one may think that their way of thinking or *mental model* is the most reliable for designing risk

communication. As mental models of experts are not the same as of non-experts this implies that experts should understand the mental models of users (Asgharpor *et al.* 2007; Wash 2010; Wash and Rader 2011; Blythe and Camp 2012). To effectively communicate the information security risks, this requires both communicating the risk and motivating the user. Hence, the validity of user's decisions arguably depend on what, when and how information is provided by the messages (Wahlberg et al. 2013).

Traditional techniques used to communicate offline risks may not be effective for online risks (Blythe et al. 2011). Many studies advice that the traditional 'one size fits all' approach to risk communication should be replaced by a targeted approach in which messages are engaging, contain the required technical and non-technical context and above all tested to ensure whether they have an effect on users or not (Blythe et al. 2011; Martin and Rice 2011; Maurer et al. 2011; Takahashi et al. 2013; Shillair et al. 2015).

To effectively communicate risks, Shillair et al.(2015) suggest that users should be classified according to their IT knowledge as Naïve or novice and experienced users. In their study, they used two approaches, an inactive learning approach and a semantic descriptive approach, to explain online safety and change user's behavior. They found that for users who lack the required knowledge in handling online threats, risk should be communicated to them by stressing on their responsibility to protect themselves along with providing some 'vicarious experience' or 'show me how' about protection measures and how to behave safely online. However, this combination should be used cautiously to avoid overwhelming the user with information. Whereas for those knowledgeable users, risk communication should focus on the technical aspects of risks as in protections that increase those that are offered by their ISPs. Hence, this is done to stress on the sense of shared responsibility and continued cautious behavior rather than just informing them of online risks. This study gives an understanding on how to best communicate risk to convince users to protect themselves. Risk is communicated by educating users to improve their self confidence in protecting themselves as well as stressing

on personal responsibility of their own protection. These two aspects were perceived in the literature as aspects that influence user's security behavior (Furnell et al. 2008; Furnell and Clarke 2012; Furnell and Moore 2014). However, the vicarious experience was offered to the participants as if an expert was sitting at the user's computer and the user watching him, thus, no guarantee that the user understood the safety tips that were given or not, or even if he at least read them. However, some thought should be given on how to enhance user's engagement and perception such as using 3D environments delivery methods.

Blythe et al. (2011) argue that warnings about information security threats are often and easily ignored due to the used terminology and timing of such warnings. They recommended that users are persuaded by risk communication messages that are tailored to particular threats they may be exposed to and delivered in a timely manner before the danger or risk takes place. Further to that, these messages must describe the danger by influencing user's mental models. This was also recommended by Asgharpor et al.(2007) when they designed two card sorting experiments to understand the mental models of experts who communicate the risks and non-experts who receive the risk communication. Their findings are consistent with the literature that experts think differently than non-experts and that risk should be communicated using users (non-expert) mental models (Wash 2010; Wash and Rader 2011; Stewart and Lacey 2012).

To best understand this aspect, its underlying concepts are explained in the following sections.

3.7.1 Learning styles

In order to achieve a good level of ISA among users, many learning mechanisms where developed such as video gaming, ISA initiatives and classroom style education (Cone et al. 2007; Sheng et al. 2010; ENISA 2010; Abawajy 2012). As learning about security is not enough, where this learning should hopefully lead to a change in behavior and actually practice it to ensure its effectiveness (Talib et al. 2010; Abawajy 2012). Further to that, as the user is

solely responsible for the protection of his information and devices and not enforced to do so, he has the flexibility to choose which ever learning approach that is most convenient to him. Talib et al. (2010) and Alarifi et al. (2012) found that the most preferred learning sources for users are by reading information security material on the web, knowledge gained at workplace and through reading news articles and advertisement in newspapers. This highlights that users are not the same and learn differently. The findings of (Talib et al. 2010) suggest that although users do not perform this learning at home on a regular basis, but almost two thirds of their sample population were found to be willing to learn about information security at home. However, each individual has his own way(s) of learning preferences and styles.

Honey and Mumford define learning styles as " *Descriptions of attitudes and behavior which determines an individual's preferred way of learning*" (Coeffield et al. 2004). Vermont defines learning styles as "*Coherent whole of learning activities that students usually employ their learning orientation and mental model of learning*" (Vermunt and Verloop 1999). Stewart and Felicetti (1992) define learning styles as " *educational conditions under which a student is most likely to learn*". Hence, learning styles are not only about what individuals learn, but actually how they prefer to learn. Thus, learning styles could be defined as an individual's preferred means of learning and gaining knowledge.

Coeffield et al. (2004) classified learning styles into five families, as in Figure 3.7.

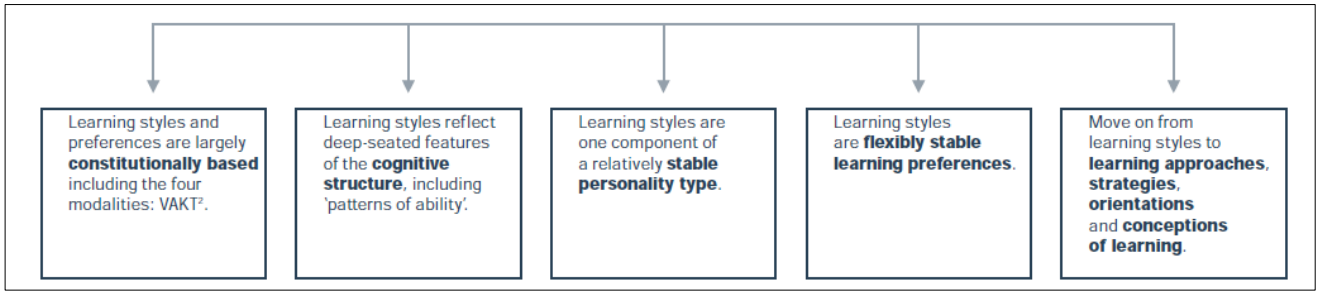

Figure 3.7: Learning Styles Families (Coeffield et al. 2004)

Many other learning styles and models exist and used by individuals to gain knowledge, where this knowledge is acquired through a number of human sensory related channels. The

most commonly used is the VAK/VARK Model represented by (Fleming 2001). According to this model, the learning styles are Visual, Auditory, Read/Write and Kinesthetic as in Figure 3.8.

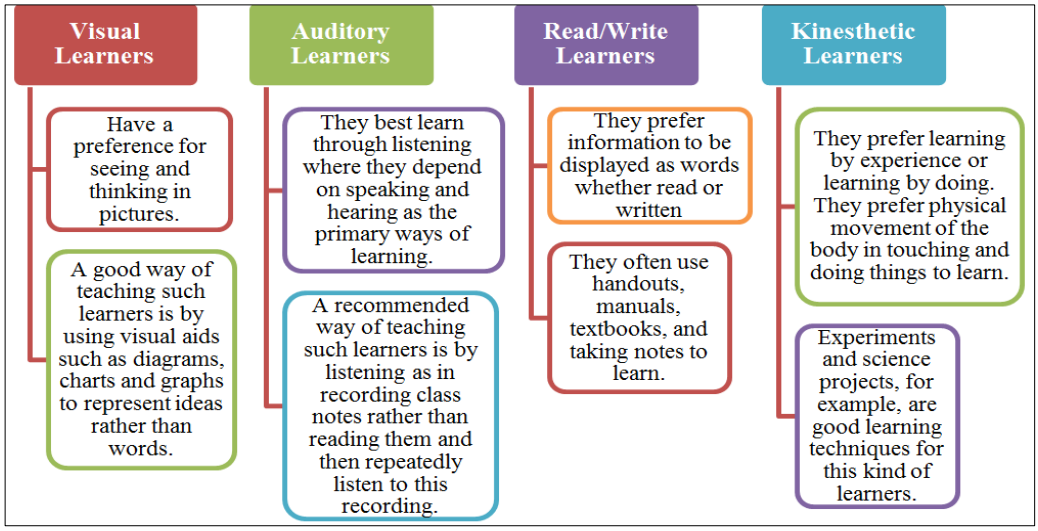

Figure 3.8: VARK Learning Styles

Individuals learn more effectively by using one of these modalities (Al Sabbagh et al. 2012). Although learning styles, especially the VAK/VARK Model are the most commonly used at schools and universities on the one hand. On the other hand, many researchers have criticized learning styles theories and questioned their validity. Coeffield et al. (2004) found that no independent research was used to adequately validate any of the most popular learning styles resulting in a conclusion that their effect on individual's learning achievement is highly questionable. This was also supported by Hargreaves (2005) where they claim that the evidence for the effectiveness of learning styles is "highly variable". Similarly, Willingham (2009) states that not enough evidence is found to support a theory that describes the learning styles differences among students.

However, as our concern is how to best raise ISA of users about information security risks and guide them to make an informed security decision , the concept of learning styles may be used as means to better communicate and improve user's understanding of information security risks.

3.7.2 Mental models and personality traits

As humans are the weakest link in information security, increased attention has been given to information security awareness and behavior in the last decade (Lebek et al. 2013). Behavioral information security focuses on human behavior to protect information systems, through awareness, from a human perspective (Lebek et al. 2013; Ophoff and Robinson 2014). This multi-disciplinary research domain, includes theories from sociology, psychology and criminology that were adapted or used by researchers to assess users' behavior and ISA (Lebek et al. 2013). These theories suggest that user's ISA of security threats influence his attitude and behavior towards these threats. However, these theories tend to assess user's intensions rather than actual behavior due to many difficulties in monitoring user's security behavior (Lebek et al. 2013). Nevertheless, a more holistic view of this challenge has to be considered to have a better understanding of how to best motivate and influence users' behavior to maximize their engagement and cooperation in the information security process.

In an attempt to understand the factors that influence information security behavior, Badie and Lashkari (2012) categorized these factors into human and organizational factors where human factors are most significant than organizational factors. Human factors were divided into factors that belong to management, workload and inadequate staffing and factors that belong to the user, lack of awareness, behavior, belief, improper technology use and lack of motivation. Similarly, Furnell and Rajendran (2012) classified human factors as workplace dependent and independent factors as in Figure 3.9.

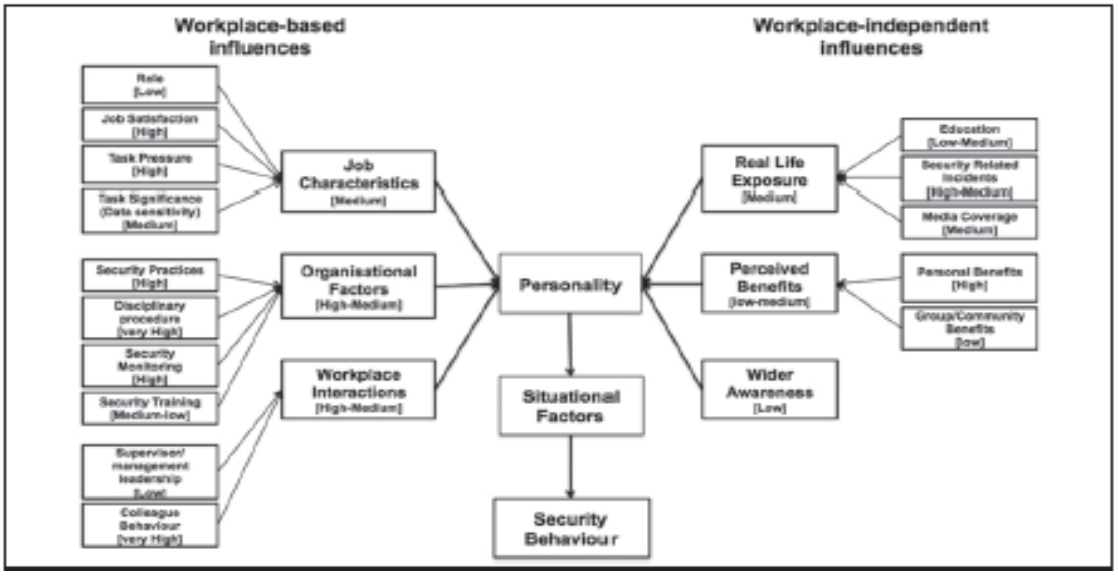

Figure 3.9: Influences upon security behavior (Furnell and Rajendran 2012)

Further to that, in their proposed model they assigned indicative weights to these factors. Although such weightings are subjective and may differ from one situation to another, but it can be used as a guide to the significance of such factor and its influence on users' security behavior. A positive aspect of this model is the consideration of a user's personality and that it contributes to information security behavior. Hence, it is not guaranteed that the same person can make the same decision in all contexts, this was reflected as situational factors. This was confirmed by (Kajzer et al. 2014; Webb et al. 2014). However, users do not respond to security threats in the same manner (Albrechtsen 2007; Furnell et al. 2008; Martin and Rice 2011; Kajzer et al. 2014) and that actual behavior may differ from intended behavior (Shropshire et al. 2015) due to various factors that are filtered through the user's personality. Hence, it is effective to further explore this aspect by considering the different personality traits and security mental models of users.

The Big Five personality traits are a widely accepted personality model in several research domains (Kajzer et al. 2014; Shropshire et al. 2015). In the information security literature, there is a trend to use the Big Five personality test to assess personality in order to understand user's behavior (Warkentin et al. 2012; Kajzer et al. 2014; Shropshire et al. 2015). The

characteristics that describe the human personality traits (Kajzer et al. 2014) are as shown in Table 3.8.

Personality Trait	Characteristics
Openness to experience	Adventurous, creative, curious and value change
Conscientiousness	Organized, rule-abiding, dependable and self-disciplined
Extra version	Energetic, sociable, place a high value on inter-personal relationships and outgoing
Agreeableness	Compassionate, kind, cooperative and likeable
Neuroticism	Insecure, angry, worrisome and impulse ridden

Table 3.8: The Big Five Personality traits

A number of studies investigated the relationship between personality traits and user's online behavior. Halevi et al (2013) examined the correlation between the Big Five personality traits and responding to phishing emails and how they relate to user's readiness to protect his privacy on Facebook. Their findings indicated that users with neuroticism personality have higher susceptibility to respond to phishing emails. Moreover, users with openness personality where found to be most vulnerable to privacy threats due to them posting more personal information on Facebook. This was confirmed by Bachrach et al. (2012) as their findings demonstrated a relationship between the Big Five and Facebook profile features. Egelman and Peer (2015a) indicated that personality traits are a weak indicator of privacy preferences compared to risk taking behavior and decision making. Hence, they proposed a Security Behavior Intentions Scale (SeBIS) to measure user's security behavior intentions. However, the reliability and efficiency of this scale requires further validation.

Kajzer et al. (2014) studied the effectiveness of some ISA message themes considering different types of individuals based on their personality traits. They used five message themes which are:

1) ***Deterrence*** which focuses on sanctions for illicit behavior.
2) ***Morality*** which focus on the user doing what is considered right.
3) ***Regret*** where prior to making a decision, individuals anticipate the consequences of their choices such as encouraging them to back up their data.
4) ***Incentive*** where rewards are given to individuals which affect choices they make.

5) ***Feedback*** received from an action, whether negative or positive, will affect individuals engagement in an action.

They used an online survey to collect data and obtained 293 usable responses. Their findings suggest that personality plays a role in the effectiveness of ISA messages and accordingly in changing a user's behavior. This indicates that to increase the effectiveness of persuasive messages, they have to be tailored to the user. Further to that, message-person congruence is highly affected by user's personality. For example, conscientiousness individuals were found to be more receptive to feedback messages while openness individuals were found to be negatively affected by regret, feedback and incentive messages. An interesting result is that older users were found to be more receptive to morality, regret and feedback messages. Further to that, individuals with more than average security knowledge were found to be negatively affected by feedback messages. This suggests that age and security knowledge have an effect on user's behavior.

In another study by Rakić-Bajić and Hedrih (2012) to explore relations between excessive use of Internet and personality traits, they found that several personality traits especially conscientiousness had a significant effect on excessive Internet use. Moreover, personality traits were used to explain the relation between user's intension and actual intensions to engage in protective behaviors and found that agreeableness and conscientiousness are conceptually linked to secure behaviors. Further to that , their findings suggest that the two constructs of the Technology Acceptance Model (TAM) which are the ease of use and perceived usefulness of security measures are significant factors that affect user's behavior. This was, similarly, confirmed by (Furnell and Rajendran 2012; Shropshire et al. 2015).

Even though some users avoid making security decisions due to lack of knowledge, skills and self-confidence, they are still required to make some decisions on a regular basis (Furnell and Clarke 2012). These decisions are arguably influenced by their mental models or how they think about information security whether these models are correct or not (Asgharpor et al.

2007; Wash and Rader 2011). Camp (2006) indicates that these mental models, as in Figure 3.10, are widely used by security experts.

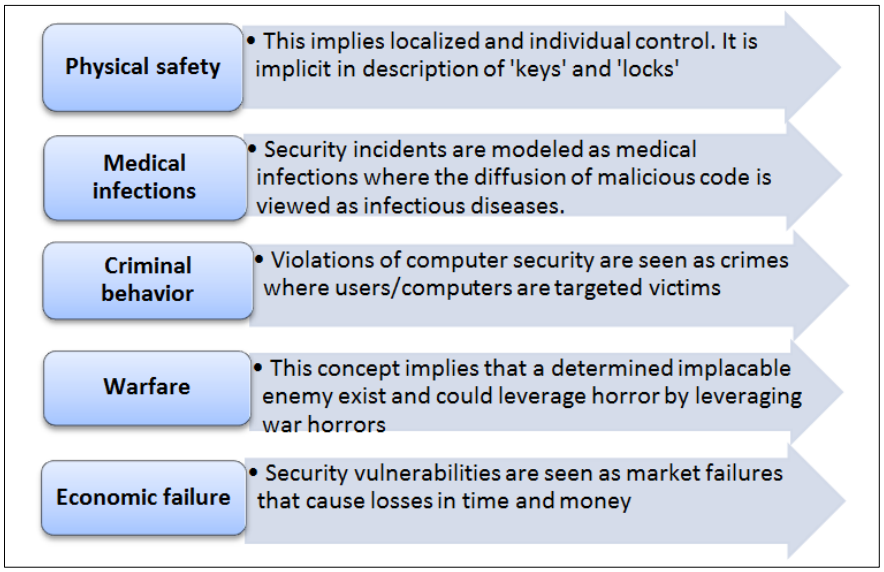

Figure 3.10: Mental Models (Camp 2006)

So, mental models could be interpreted as psychological representations of hypothetical, real or imaginary situations. They describe how an individual reason about a situation or a problem, make predictions about what might happen and provide guidelines on which behavioral choices are based. They develop and change over time adapting to new experiences and information (Asgharpor et al. 2007; Wash 2010; Wash and Rader 2011). Each mental model can result in a different user response such as physical mental model evokes lock-down and protection responses (Camp 2006). Accordingly, to understand user's behavior, one needs to understand how he thinks.

To better understand mental models used by HU to make security decisions, (Wash 2010) interviewed 33 non expert HU. By focusing on differences between users, he identified eight mental models that could be divided into two categories:

- Models about spyware, adware, viruses and other forms malware as they did not distinguish between them (medical infections mental model)

- Models about attackers and the threat of breaking into computer where they used the term 'hacker' to describe anyone who does bad things on the Internet regardless of who they are and how they work (criminal behavior mental model).

These findings come consistent with (Harbach et al. 2014) that user's top security concerns are about privacy, account abuse, malware, hackers and financial risks and fraud. However, their findings demonstrate that there is a difference between expert and non-expert mental models and how these models affect the HU security behavior. This was also confirmed by (Asgharpor et al. 2012).

In a following study, Wash and Rader (2011) tried to explore the sources of information, where these models, whether correct or not, come from and how they impact these mental models and found that shared security stories and experiences are the main sources of information. As stories shared by people among the community, media, personal experience will lead to change the way users think about security and by focusing on models that lead to better decisions rather than which models are correct, they propose a new way of thinking about users' security. However, sharing stories is not enough, but sharing the right stories is needed. This is achieved by having a community based story repository that is monitored by IT experts where only stories that lead to a positive information security behavior are included. A similar approach to create a community based risk repository was also recommended by (Van Cleef 2010).

3.7.3 ISA Delivery methods

Attackers often focus on the vulnerabilities created by human factors as it is considered the least resistant path (Abawajy 2012). Despite that ISA is considered to be one of the defense lines against information security threats (Aloul 2010; Abawajy 2012; Alarifi et al. 2012; Al-Hadadi and Al Shihani 2013; Kaur and Mustafa 2013) it is not a final goal, but should go beyond to changing user's behavior towards information security. Some of the critical success factors of ISA is the delivered message to the user, why and how it is delivered (Sheng et al. 2010; Khan et al. 2011; Abawajy 2012; Sedinic et al. 2014). There are many types of ISA

delivery methods ranging from classroom-style workshops to web based training as in Table 3.11. In reference to Table 3.9, several studies in the literature have discussed the effectiveness of such delivery methods, user's preference and how they are used.

Researcher	Effective Delivery Method(s)
Sheng et al (2010)	Online game (Anti-Phishing Phil) and a comic (PhishGuru)
(Albrechtsen and Hovden (2010); Khan et al. (2011)	- Workshops, dialogue and group discussion
Abawajy (2012); Al Sabbagh et al. (2012)	Video based training
Alarifi et al. (2012)	Web portals, newspapers and advertisement
Sedinic et al. (2014)	Web based training
Olusegun and Ithnin (2013)	Emails, monthly newsletters, advertisement in newspapers, presentations, posters, payroll stuffers and web based and in-person training
Sari and Prasetio (2017)	Electronic word of mouth (Knowledge sharing in social networks)

Table 3.9: Effective Delivery Methods

For example, Albrechtsen and Hovden (2010) discussed and evaluated the effects of a training program that involves users directly to improve their ISA and behavior. Their findings suggest that behavior is a direct product of ISA and that it takes more time to change behavior than ISA and that information security dialogue and the sharing of security experiences is an effective approach to increasing ISA and behavioral change. This is confirmed by findings of Wash and Rader (2011). Nevertheless, this study fails to show how effective is this approach compared with other delivery methods.

Olusegun and Ithnin (2013) implemented a campus wide ISA program to educate staff, faculty members and university students about information security. For students, emails, monthly newsletters, advertisement in students' newspapers, presentations, posters and web based training delivery methods were used. Whereas for faculty and staff members, they used in-person and web based training, posters, monthly newsletter, payroll stuffers and targeted emails. The only metric used to measure the success of the program was the increase in the number of reported incidents regarding threats to information assets and viruses which shows that the targeted audience were receptive to this program especially that the training part was not compulsory. However, no information was given about the existence of a university

security policy and whether students and non-students were aware of it. A good idea was to put the security policy in a poster or at least a link to it on the university's website.

To study the relationship between phishing susceptibility and demographics as well as the effectiveness of several anti-phishing education material, Sheng et al. (2010) conducted an online study. Participants knowledge about phishing was assessed by them answering survey questions then engage in a role-playing game. Later, they received some education about phishing then finally played a second round of the role-playing game. Among their findings, participants fell for 47% of given phishing websites prior training that decreased to 28% after receiving the anti-phishing education. These findings suggest that awareness of phishing and how to avoid it could be learnt from training materials such as games and comics. As participants behavior was assessed before and after the training, their findings give strong indications on the effectiveness of the delivery methods used.

Currently, social networks/media are becoming a useful platform for enabling knowledge sharing whether on personal or organizational level. Due to its increasing popularity, social networks could be utilized as an effective online learning community and a tool to educate users about information security (Tayouri 2015; Chan et al. 2016; Ahmed et al. 2018). To reflect on the preference of social networks as an ISA delivery method, Shillair (2016) conducted an online survey that attracted 800 participants. Among its findings is that the majority of participants saw social networks as a good source of security awareness and training that could help enhance online security and safety. Several studies have sought to explore the effectiveness of utilizing social networks in raising ISA and their findings are encouraging (Labuschange et al. 2011; Cetto et al. 2014; Chan et al. 2016; Karavaras et al. 2016). Motivated by the massive use of social media, Sari and Prasetio (2017) for example, investigated the effectiveness of group discussion to share knowledge in social networks called electronic Word of Mouth (eWOM). In this method, users exchange knowledge through informal communication. They used an online survey for data collection. Among their findings was that on respondents Timeline, 82% believed the security articles shared by their friends and

72% will retweet/share these articles suggesting the popularity of this kind of delivery method. However, nothing was mentioned regarding the trusting of information source.

Similar studies have shown user's preference of delivery methods such as web based training (Sedinic et al. 2014), video based training (Abawajy 2012; Al Sabbagh et al. 2012), group discussion and workshop (Albrechtsen and Hovden 2010; Khan et al. 2011) and web portals, newspapers and advertisement (Alarifi et al. 2012).

In a study by Abawajy (2012) to compare the effectiveness of text based (short web articles), video based ("how to avoid phishing" video) and game based (Anti-phishing phil) delivery methods, a qualitative experiment was conducted where participants of different demographics and varying levels of ISA were chosen. However the text based and video based methods where to found to better broaden the participants knowledge in their ISA compared to game based methods. Moreover, over 50% of participants preferred video based methods and over 33% preferred text based methods whereas only 5% preferred game based delivery methods. These findings may be surprising, but one could explain the high preference of video based methods due to the clear and easier to follow information. Additionally, this could be due to lack of interest in reading an author's predetermined structure article and to better understanding of concepts and ideas when presented in both visual and verbal form. The low preference of game based methods could be correlated with participants demographics which were not explained in this study. However, the effectiveness of each of the selected delivery methods varied. This indicates that to maximize the benefits of an ISA effort, a joint approach should be used that utilizes a combination of delivery methods rather than focusing on one. This is consistent with findings of (Shaw et al. 2009; Albrechtsen and Hovden 2010; Khan et al. 2011; Al Sabbagh et al. 2012). This is may be due to the use of more than one human sensory learning styles at the same time in presenting information.

Khan et al. (2011) assessed the effectiveness of ISA delivery methods from a psychological perspective. Delivery methods effectiveness was evaluated on the basis of their proposed five

step ladder model. This model resulted from the integration of the Theory of Planned Behavior (TPB) and the Knowledge, Attitude, Behavior (KAB) model. They assessed seven ISA delivery methods according to the presence or absence of their model's components. Results are as shown in Table 3.10.

S/No.	Tool and technique	Component of knowledge	Component of attitude change	Component of subjective norms	Component of Intention	Change in behavior	Overall effectiveness
1	Education presentation	✓	✓	x	✓	✓	4
2	Email messaging	✓	✓	x	✓	x	3
3	Group discussion	✓	✓	✓	✓	✓	5
4	Newsletters	✓	✓	x	x	x	2
5	Video games	x	✓	x	✓	x	2
6	CBT	✓	✓	x	x	x	2
7	Posters	✓	✓	x	x	x	2

Table 3.10: Effectiveness of ISA Methods (Khan et al. 2011)

The most effective delivery method was the group discussion which is similar to (Albrechtsen and Hovden 2010) findings. However, this is an ISA theoretical study based on awareness and behavior psychological theories. Although their findings are confirmed by literature (Albrechtsen and Hovden 2010), but these findings would have been more comprehensive and indicative if backed up with experimental evidence.

	Delivery Method	Comments	Pros	Cons
Conventional	Paper based	Such as posters, brochures, and newsletters	- Highlight timely sensitive issues - Periodic ISA enforcement - Targeted audience can be easily reached	- Could be easily lost and overlooked - Needs proper distribution - Relevant to targeted audience only
	Trinkets	Such as pens, notepads where a security message is attached to it	- Cost effective to produce	- Convey a single message - Message has to be well written
	Electronic based	Security alert messages Such as screen savers and pre-logon messages	- People are guaranteed to see it because it is placed on the computer	- Does not reach those without computers
Instructor-led	Classroom-style workshops and group discussions	Knowledge and experience is shared among participants under the monitoring role of the IT expert	- Interactive with the engagement of all participants - Answers are provided in a timely manner	- Fairly expensive - Boring if participants are not motivated to share their experiences and knowledge
	Seminars and educational presentations	A formal approach to ISA where an IT expert is used to lecture users	- Reach a large population - Face to face communication	- Boring - Instructor has to have an ability to engage participants
Online	Email broadcasts	Developed by organizations or by IT experts	- Cheap - May convey more than one message - Directed at targeted audiences	- Targeted audience email addresses have to be known - May be undermined due to spam
	Blogs and websites		- Can be timely and updated	- Users may not be aware of them - May not include the proper guidance.
	Web-based training	Enable users to improve their knowledge at their own pace	- User friendly - Can reach a wider audience regardless of their geographical location - More detailed content	- Expensive to be developed - Requires some technical knowledge in advance - No interaction with trainee
	Social media	A popular mobile learning platform	- Message can be monitored if audience liked it or not	- Message has to be engaging and appealing to users
Game based	Edutainment games	Catches the player's attention and engages him. A good way for motivating the user to adapt the desired behavior	- Interactive - Appealing to certain groups such as the young	- Has to be carefully designed to ensure its objectives - Effective only if taken seriously
Simulation based	Embedded training	Simulated phishing emails sent to users to test their vulnerability to phishing attacks followed by training	- Learning by experience	- Users must have a technical knowledge in advance.
Video based	Educational videos	Combine audio and visual learning	- Easy to use - Users can start and stop it at anytime - Flexible, can be watched several times	- Cannot guarantee content absorption - Expensive to develop

Table 3.11: Classification of Delivery Methods

3.8 Discussion

Users should be equipped properly to be protected. It is not enough to know about threats and why they are significant, for example, but they should be able to know what to do to protect themselves from these threats and how to use the related safeguards. This implies that the approach to awareness needs to be changed from just informing users about security issues to actually helping them to develop the ability to deal with them, i.e. create an information security literacy among users by creating a baseline of information security culture (Kritzinger and von Solms 2010; Furnell and Clarke 2012; Furnell and Moore 2014; Kritzinger and Von Solms 2013).

Users, arguably, do not have the time or willingness to educate themselves about information security (Talib et al. 2010; Maurer et al. 2011). Additionally, they may be faced with difficulties in "*how to do"* things practically due to differences between devices, systems and platforms used (Furnell and Moore 2014). Indeed, users have problems in understanding the security functionality of some standard applications and tools such as web browsers and email software (Rao and Pati 2012). This could be due to the fact that information security software developers have assumed users possess too much prior knowledge and, thus, failed to assist and inform the user in making security related decisions (Aloul 2010; Furnell and Clarke 2012).

If users lack the required knowledge or not prepared to make such decisions, this may result in weakening the performance of the proposed control (Furnell and Clarke 2012). Eventually, the successful operation of such tools depend on how the users' deploy, configure and operate them (Talib et al.2010). Even younger people who grew up with technology and are significant users of it were found to be not using it properly (Furnell and Moore 2014) which highlights the importance of an ISA approach that goes beyond informing the user, to convincing the user of his responsibility for his own protection and providing him with the needed guidance on what to do to be protected.

To overcome this challenge, a number of approaches could be used. These are automation, education, understand how the user think and a joint approach:

As it is argued that users are not well equipped or "ill-informed" to make the proper security decisions when needed (Kritzinger and von Solms 2010; Furnell and Clarke 2012; Furnell and Moore 2014), then increasing the level of automation in security software maybe a solution. This implies that the user is removed from the decision making process in security solutions that are targeted for HU and, thus, making the security software act more securely (Furnell et al. 2008; Wash and Rader 2011; Furnell and Clarke 2012; Rao and Pati 2012). This "Stupid User Approach" (Wash and Rader 2011) is quite successful. Many modern Firewalls operate securely without user intervention. Anti-Virus software, for example, has minimum interactivity with the user as it regularly and automatically scan the computer for known malware and remove it. Microsoft, in Windows 10, is replacing the scheduled monthly updates used in older versions of Windows to automatic updates whenever needed (Microsoft.com 2017). Moreover, a security software may integrate more than one functionality such as Norton Internet Security suite that provides Anti-Virus protection, Intrusion Detection and warns the user about known unsafe websites before visiting them. Further to that, this approach has inspired the authors of (Rao and Pati 2012) to recommend the development of an intelligent software that automates the responses to some web browsers' features such as ActiveX controls and cookies. This is done by tracking the preinstalled software on the user's system and user's Internet behavior then this intelligent software is tuned accordingly to provide protection with little user intervention. As this *Automation Approach* may be attractive, but it has limited effectiveness where some modern threats are difficult to protect from by technology only. Good examples of such threats are phishing and social engineering threats (Aloul 2010; Hasan and Hussin 2010; Sheng et al. 2010). Furthermore, a software update for example, may not be compatible with a user's preinstalled favorite software or resource such as

RAM which may result in him simply rejecting this update. This is the case where ISA is crucially needed for the user to appreciate the nature of security threats and motivate him to make an informed decision. An extension to this approach is the one recommended by (Furnell et al. 2008) where the user is required to have the appropriate security controls installed and updated before granting the system full functionality to operate online. However, this may not be feasible and less realistic as it would unfairly put demands that are arguably not understood by the average user as it requires major information security culture change. Another idea for enforcing users to protect themselves is by delegating the user's protection to an ISP (Kritzinger and von Solms 2010; Kritzinger and Von Solms 2013).

Another extreme to the former approach is to give the user the freedom to choose based upon appropriate information security training so he has the ability to make an informed decision, or the " *The Education Approach*" according to (Wash and Rader 2011). Motivated by this approach, the authors of (Wahlberg et al. 2013) proposed a web browser Google Chrome Add On, named Kepler, to raise browser security awareness and help users find out what is actually happening during web browsing such as where resources are requested from and what kind of responses were returned in an appealing "eye-pleasant" format to satisfy as bigger audience as possible. Moreover, it provides information about the security of the request to non-technical users in a clear and understood way. This way users can make security decisions by themselves. As Kepler may be considered as a step forward in informing and educating the user by presenting detailed information about web browsing in a human, easily readable form, it is just a prototype. Thus, no real indications exist about its functionality yet. But it was worth reviewing due to its original concept in educating users about web browsing and giving them the freedom to choose. However, a drawback of this prototype is that when results are displayed to the user, no filtering of requests is made which might leave the user confused between harmful and non-harmful request. This *education* approach can be translated into information security training and education for organizational employees and

the different ISA initiatives made by Governments, Operating System vendors and Anti-Virus providers that were discussed earlier. However, for the general public this may arguably be challenging especially that little evidence is found that HU are knowledgeable of information security and actually practicing it (Talib et al. 2010). This confirms the need that users should gain ISA at a younger age by having schools integrate information security in their curriculum to teach them about different information security issues and their responsibility in how to protect themselves against information security threats. Not limited to that, but also teach them about the ethical and legal aspects of online behavior (Hasan and Hussin 2010). Although this may not result in a perfectly aware population but will help in having individuals that are better aware of the current situation and how to respond to it.

A recent approach is the "*understand how the user think approach*" (Wash and Rader 2011). This is a more complicated approach as it requires to understand how users think about information security and how they make security decisions. This approach may be inspired from facts that IT experts overestimate the net value of security and ignore users' efforts and time spent when giving advice to them. Moreover, users tend to ask family and friends for advice on security issues rather than formal support from experts and official online resources (Furnell et al. 2008; Furnell and Clarke 2012). The authors of (Wash and Rader 2011) believe that one of the promising approaches to improve user's ISA and change his behavior accordingly is through changing his mental model, i.e. the way he thinks about security, by providing a mechanism for non-technical users to sharing security stories with each other. This may be a good approach to influence users' behavior as it is successful in other disciplines, i.e. the healthcare, but a major drawback of this approach is that users may not be willing to share highly personal and sensitive information about information security incidents. Further to that, they may not see such stories as beneficial to others or they may report more security behavior than reality just to give the impression that they are more secure than they really are.

A *joint effort* approach in which many groups work together to produce a security-minded individual. Whereas home computers are used by attackers as platforms, , i.e. botnets, to launch attacks such as DDos attacks on a country's or other countries information infrastructure (Kritzinger and Von Solms 2013), cyber security laws should be produced and enforced by Governments. As these threats are not limited to one country, there has to be some form of collaboration between Governments around the world to fight against cybercrime. Additionally, Computer Emergency Response Teams (CERT) should be established to improve the ISA among users. Computer forensic teams should be established in police departments to aid in catching such attackers. Even Non-Government organizations should launch ISA and education campaigns to their employees and to users from the general public as a community service and assess its effectiveness. Advice on how to safely use the Internet should be provided by Internet Service Providers (ISP). The media also has its role in this joint effort by continuously publishing information about information security incidents together with the penalty put on attackers. Last but not least is the users themselves, by sensing the responsibility and their role in being part of the solution and continuously be aware of information security threats and how to combat them through educating themselves.

Thus, when educating the user and directing his behavior several aspects should be considered to leverage the learning process. The following are found to be key behavioral influencers:

1) **Different learning styles** should be considered to increase user's engagement into the learning process and, thus, increase the learning outcome. For example, in a visual /audio learning style, more images, color, pictures and other visual media could be incorporated along with some background sound to increase the visualization.
2) **Cultural differences** is another aspect that has been found to affect user's behavior. Users come from different countries of different cultures. Hence, what sounds like a good learning mechanism for some users from a certain culture may not be suitable for another

user from another culture. Therefore, understanding how users from different countries and different cultural backgrounds perceive Information security and manage it accordingly affects the shaping of their behavior especially with the existence of culture-specific risks.

3) **Level of IT expertise** has a significant effect on user's behavior whereas this expertise is obtained through formal information security education such as in IT experts. This should be highly considered especially when communicating risk to users to both persuade them and avoid overwhelming them with information already known to them. However, the higher the level of IT knowledge does not guarantee secure behavior. This is evident as in young people who are significant users of technology are not found to be good users of it especially regarding their behavior in Social Networks and their tendency to reveal sensitive information such as photos and location (Hasan and Hussin 2010; Furnell and Moore 2014).

4) **Awareness** of information security risks, as users, who are found to be ill-informed, and their arguably lack of awareness is one of the reasons behind them becoming the weakest link in information security. Eventually, users can only pay attention to risks they are aware of and act accordingly (Albrechtsen 2007). Knowing which information security risks users want to be protected from is significant in convincing them to protect themselves. However, according to the KAB model, knowledge accumulation leads to a change in attitude and, therefore, a change in behavior (Khan et al. 2011). Thus, an increase of knowledge may not be the ultimate factor, alone, of behavioral change on the long term. This aspect could be more explained by focusing on the factors that cause a change in attitude and result in direct or indirect change in behavior. Subjective norms or the user's belief of what people think about him, is another factor that causes a change in behavior through the awareness component. According to Theory of Planned Behavior (TPB), behavioral change depends on individual's intensions. These two factors, attitude

and subjective norm, are correlated where a positive attitude and subjective norms have a positive influence on intentions to change a behavior (Khan et al. 2011). Moreover, stressing on personal responsibility and that users are solely responsible for the protection of their own information and devices along with the required guidance on how to protect themselves has an effect on their behavior. Lack of awareness is considered a vulnerability that can be exploited by attackers such as phishing attacks. As one of the goals of ISA is to reduce information security risks, a proposed way to assess such ISA is that after educating the user, he may be asked some questions to assess his material absorption. However, answering such questions correctly does not guarantee that the user is motivated to change his behavior according to the accumulated knowledge. One solution to that is to have an automatic security reporting incident database. The lower the number of unsolved reported incidents, the higher the ISA level.

5) **Usability (perceived benefit and ease of use)**. Since HU have no security policy to comply to, but have guidelines instead, negative consequences are the only punishment they may have to fear. Technology does help them in providing some level of protection but technology alone is no silver bullet. Accordingly, one way to motivate users to adopt positive security behavior is by convincing them to prevent such negative consequences by utilizing security countermeasures. Further to that, users find some difficulties in using security tools which may be an obstacle in them adopting such tools. As software developers assume way too much knowledge in users when designing their tools (Wash and Rader 2011; Furnell and Clarke 2012; Stewart and Lacey 2012) this may result in users having difficulties in understanding how these tools work. This misunderstanding may result in them degrading the tools performance or simply shutting it down especially if it continues to bother them with annoying messages, reduce their productivity or conflict with other favorite software. Another problem with security software is that the benefits of

using it may not be evident or noticed as other software that enhance user's performance and have a clear functionality such as word processors and spreadsheet applications. Therefore, users have to discover a security measure first, and then decide if it is worth the effort to use it or not (Harbach et al. 2014).

6) **Past experience**. This experience, whether correct or not, of information security risks creates a level of ISA that is gained informally from several resources. Examples of such resources are security stories from family and friends, media coverage or previous security incidents.

7) **Risk communication**. Effective risk communication attempts to change user's risk perception to elicit safe behavior. As risk is perceived differently among users (Albrechtsen 2007), it is important to have targeted risk communication to ensure its relevancy (Blythe et al. 2011; Maurer et al. 2011; Wash and Rader 2011; Al Sabbagh et al. 2012; Stewart and Lacey 2012; Harbach et al. 2014). The problem with risk communication is that it is designed by experts who communicate facts about risks and them being experts in technology does not guarantee that they can best communicate the risk. The approach to risk communication should arguably be user focused and not fact focused (Stewart and Lacey 2012). That is, messages are tailored to user's needs and understanding. Ineffective risk communication may result in negative consequences that experts blame users for. Experts often use words like 'stupid' or 'lazy' (Wash and Rader 2011; Abawajy 2012; Rughiniş and Rughiniş 2014) to explain users' behavior and overlook limitations that are placed on them such as time, resources, money and learning capabilities. However, when users respond to risk this does not imply they are guaranteed to make the right choice or do the best practice. This highlights the importance of considering limitations opposed on users who may not arguably look for a 'perfect choice' as modeled by experts, but for a choice that satisfy their needs and limitations. This is

evident when risk communication messages use technical terminology that may not be well understood by users, resulting in them choosing an option related to his understanding of the situation. The key to effective risk communication is to communicate the right information at the right time and framed in the right context. More effective risk communication and behavioral change can be developed by classifying users as discussed in section 3.5 or by considering personality traits of users (Kajzer et al. 2014). Instead of having traditional pop up boxes with words that are often too technical to comprehend by the user and to ensure the proper influence, risk communication has to be tailored to specific needs of users. To avoid overwhelming the user, the message should be proactive, simply worded where jargon and technical terminology is tailored to his IT level, state the risk, why it is relevant, what to do and finally how to protect from that risk. This is done to arguably ensure a long term outcome. Additionally, messages have to be relevant, timely, up-to-date to reflect the evolving threat landscape, guiding with an interesting delivery mechanism. However, the design of such messages has to be done carefully to avoid negative influences. This will arguably maximize message appeal and persuade users to change their behavior to take an informed action.

8) **Mental models**. These are user's understanding of a situation and how they think about it and act accordingly. As experts' mental models are different form non-experts, it is significant to understand user's mental models and how they perceive the risk in order to motivate them to change their behavior. By understanding their mental models, it may be possible to identify and explain the reason(s) behind such behavior. Instead of just communicating general facts about risks, targeted communication that try to alter these behaviors or reasons behind such actions may arguably be more efficient and effective. This may play a role in designing messages that are within the arguably limited cognitive skills of the user.

9) **Personality traits**. These are factors that affect user's behavior and unethical computing practices. Different versions of the same message, by using the manipulation of words, could be used to have different effects on different personalities (Kajzer et al. 2014). Hence a change in behavior could be achieved if a message is framed towards the user's personality trait. By simply having a user undertake a personality test by answering some questions, his personality trait will be identified and the message will be framed accordingly.

One of the objectives of this research is to raise user's ISA and change his behavior accordingly especially that users may be aware of risks but simply choose to do nothing about them. The above mentioned factors were found to be key influencers on user's security behavior. As in Figure 3.11, factors from 1-7 are all filtered through the user's personality then results in a change of user's behavior or reinforce good security practices. Given that users have limitations that affect their behavior and may not make the same security decisions in the same situations all the time resulting in some users being at risk more than others.

3.9 Conclusion

Attackers often choose the least resistant path of unintentional vulnerabilities created by the human factor but information security is as strong as its weakest link. As users are found to be lacking ISA in general due to many reasons, it is important to continuously raise their ISA to transform them from ill-informed users to security minded users. However, this transformation could be achieved through a number of identified critical success factors that influence users' behavior. A user needs to know the risk, understand the need to act against it and change his behavior accordingly to make an informed decision. Indeed, raising ISA and having a security minded user is not easy. This is evident as many ISA raising initiatives have been undertaken and many solutions and counter measures are proposed and users still show low levels of ISA.

However, there is no right or wrong ISA as it is not a single step but a continuous journey to raise users' responsibility in protecting themselves and be capable of detecting, removing threats and making informed decisions when required. As it is challenging to meet the needs of every user, this could be achieved through a structured approach to ISA by knowing how aware users are of security risks, the extent in which they make security informed decisions and why certain users are "at risk" more than others and the reasons behind that.

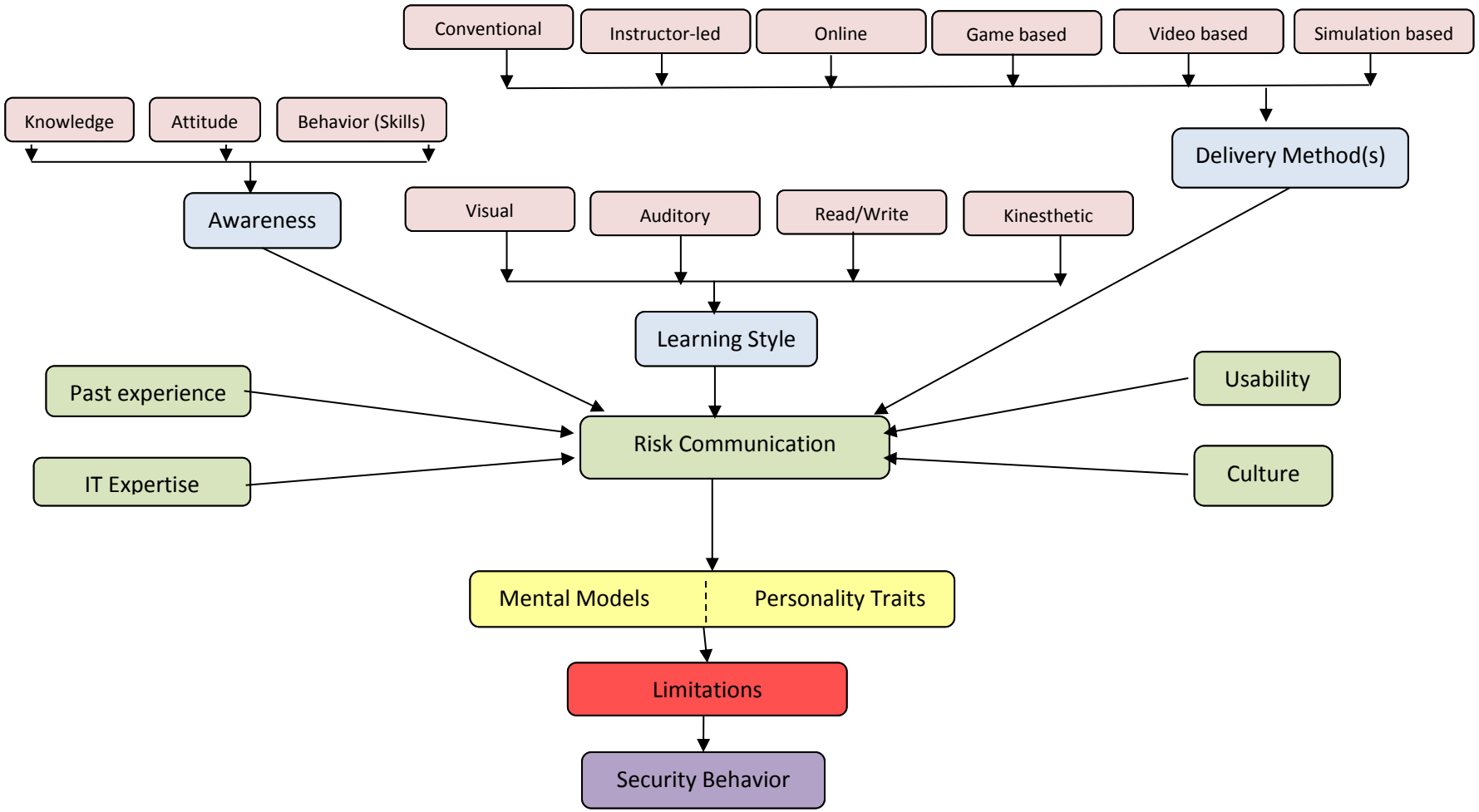

Figure 3.11: Key Behavioral Influencers on User's Security Behavior

Chapter 4 : An Investigation into the Impact of Personality, Demographics, IT expertise and Service Usage on End-users' Security Behavior

4.1 Introduction

Identifying the characteristics that may influence end-user's security behavior and being highly vulnerable to security threats is an important step in protecting and defending such users against security attacks. Additionally, as end-users' intentions may differ from their actual behavior and the fact that different users react differently to the same stimuli, it is imperative to understand the extent in which end-users are practicing good security behavior and the reasons behind these variations in security practices. Therefore, knowing how this behavior is influenced by user differences and to what extent, will help in designing solutions that adapt to the needs of those who are vulnerable.

This chapter is structured as follows: related work is described in the next section followed by the Research Methodology. Findings of the survey are presented in Section 4. The significance testing on the relationship between user-centric factors and the risk taking behavior is examined in Section 5 followed by a discussion of the main findings of the study and a conclusion in sections 6 and 7 respectively.

4.2 Related Work

Despite the interest of studying user's security behavior and practices, correlating it to psychological factors, demographics and other characteristics has not been thoroughly explored yet. Demographics, include age, gender, education level, and occupation, are the most common characteristics that are often used to analyze behaviors. For example, the password is the most common protection method for end-users' systems and data. Bonneau (2012) has demonstrated that

the strength of the password is associated with end-users' age (i.e., older users tend to use more complex password) and their nationalities. Schuessler and Hite (2014) suggest that a user's password strength is affected by their educational background and work ethic. Butler and Butler (2014) undertook a survey of 737 respondents to explore other factors have suggested that poor password behavior could be caused by the lack of user's knowledge and motivation. From the attacking perspective, social engineering is a simple yet effective attack that is widely used to obtain end-users' information, such as login credentials. Workman (2007) demonstrates that social engineering victims shared several common factors (e.g., age, education, and commitment). Also, Sheng et al. (2010) suggest that gender and age are two key indicators that can be used to predict end-users' phishing susceptibility as they found that female participants aged 18-25 were more vulnerable to phishing attacks. From a training and education perspective, Jeske et al. (2014) suggest that a user's IT proficiency was in line with their security decisions; and hence better security decisions can be made if user's IT proficiency was improved. By studying the impact of cultural factors on user's security awareness levels, Kruger et al. (2011) demonstrate that the user's security awareness levels are related with their language, gender and fields of study. Further to that, the real time behavior and the ability to defend against real time threats in users who are either more aware of Internet risks or use the Internet more than others, depended on factors other than security awareness such as individual differences that needed further investigation (Halevi et al. 2013).

Moreover, empirical evidence, through personality psychology, was found that the study of personality explains differences in human behavior (Oliveira et al. 2013). The use of personality to understand user's behavior is a well-established domain. In order to obtain a person's personality characteristics, a number of test models can be utilized, such as the Revised NEO Personality Inventory (Costa and McCrae 1992), Five-Factor Model Rating Form (Lynam and Widiger 2001), and Ten-Item Personality Inventory (Gosling et al. 2003). Amongst these models, John and

Srivastava's (1999) 44-item Big Five Inventory (BFI) model is one of the most widely accepted and used across several research domains. The BFI model contains 5 main set of personality traits: extraversion, agreeableness, conscientiousness, neuroticism, and openness to experience (Costa and McCrae 1992).

The use of personality factors to predict and explain various IT security behavior was initially proposed by Shropshire et al. (2006). However, they only theoretically discussed the ability of two personalities (i.e., conscientiousness and agreeableness) to predict user's IT security compliant behavior. Since then, several research works have been conducted in this area. Based upon empirical results, Gabriel and Furnell (2011) demonstrate that 8 personality facets show strong correlation with end-user's generic security behavior, for example, imagination facet and user's security behavior have positive correlation while the immoderation facet and user's security behavior have a negative correlation. Schuessler and Hite (2014) suggest that both agreeableness and neuroticism are negatively related with user's password strength while extroversion shows a positive correlation. Shropshire et al. (2015) claim that the connection between user's behavioral intent and use of security software can be moderated by agreeableness and conscientiousness; while Uffen et al. (2013) investigated the influence of personality upon smartphone users' opinions upon the effectiveness of security mechanisms specifically. Their experimental results suggested that both openness and conscientiousness have positive correlation upon user's intentions to utilize smartphone security controls while neuroticism has a negative one. Kajzer et al. (2014) suggest that a best fit security awareness theme can be introduced based upon user's personality, hence, potentially improving the user's IT security proficiency.

For the attacking perspective, a couple of studies have investigated the impact of personality upon end-users' behavior on phishing emails. Halevi et al. (2013) demonstrate that a high correlation was found between the neuroticism and responding to phishing attacks. Meanwhile,

Pattinson et al. (2012) show that openness, extraversion, and agreeableness were related with user's actions when dealing with the same situation. From the Organizational point of view, a number of studies demonstrated some evidence that personalities can influence security policy compliance (Herath and Rao 2009; Hu et al. 2012; McBride et al. 2012; Johnston et al. 2016) and potential insider misuse (Warkentin et al. 2012).

Prior work on investigating the relationship between various factors and user's security behaviors is already established; and a summary of existing studies is presented in Table 4.1. Nonetheless, a number of limitations are observed from these studies, including the low number of participants (e.g., Kruger et al. 2011 and McBride et al. 2012) and factors being considered mainly focused on demographics (e.g., Workman 2007). Moreover, Gabriel and Furnell (2011) concentrated on personalities only while Hu et al. (2012) targeted on the impact of top management and organizational culture. Additional limitations are limited user security behaviors (e.g., phishing (Sheng *et al.* 2010) and password practice (Schuessler and Hite 2014)). This implies that individual variations in the process of risk taking behavior is influenced by a number of several factors that may give a deeper understanding of how users understand security risks and behave accordingly.

Therefore, a study that investigates the effect of these variations on user's information security behavior and the relationship between user's security behavior and differentiating factors from a holistic perspective is required. This would provide a deeper insight into variety of affecting factors and risk taking behavior. It could be used to predict their security behavior risk level, i.e. more or less likely to engage in good security behavior than others, and design solutions that account for these individual differences instead of the traditional "one-size-fits-all" solution.

Studies	Focus	Outcomes	Method	No. of participants
Workman (2007)	Investigates reasons why people may fall victim of social engineering attacks	Results demonstrate social engineering victims share several common factors (including age, education, and trust)	Regression	588
Herath and Rao (2009)	Assess the impact of organization's commitment upon employee's intentions with security compliance	Suggest that self-efficacy is a strong indicator of user's intentions regarding policy compliance	Correlation and a component-based approach of Partial Least Square (PLS)	312
Sheng et al. (2010)	Investigate the relationship between phishing susceptibility and demographics	Both gender and age can be used to predict a user's weakness in phishing	Multivariate linear regression	1001
Kruger et al. (2011)	Study the impact of culture in user's IT security awareness	Mother tongue has an impact on security awareness level	ANOVA test	180
Gabriel and Furnell (2011)	Investigate the connection between user's security behavior and their personalities	8 personality facets showing strong correlation with user's security behavior	Pearson correlation	20
Hu et al. (2012)	Investigate a number of factors on how to manage employee to comply with InfoSec policies	Demonstrate that conscientiousness has a significantly positive effect on the user's intention on InfoSec polices compliance	A component-based approach of PLS	148
McBride et al. (2012)	Investigate the impact of situational factors and personality traits upon policy violation within the InfoSec domain	Confirms that users respond to same security scenarios different due to their personality traits	General linear mixed model analysis	150
Pattinson et al. (2012)	Study whether personalities have impact on how people mange phishing emails	When dealing with phishing emails, openness and extraversion are associated with not-informed users while agreeableness is related with informed users.	Spearman's correlation	117
Warkentin et al. (2012)	An investigation of individual personalities on insider abuse intentions	Their results confirm that personalities have impacts upon individual's cybersecurity behavior	Random Intercept Model	86
Halevi et al. (2013)	Study how user's personality traits contributed to their cyber security and privacy practice	The correlation between the neurosis trait and user's responding to phishing attacks is high	Bi-variate Pearson correlation	100
Uffen et al. (2013)	Explore the influence of personality has upon smartphone users' opinions on the effectiveness of a security mechanism	Their outcomes indicate that some personalities influence how security controls are used by the user	A component-based approach of PLS	435
Jeske et al. (2014)	Explore the relationship between IT proficiency, impulse control and secure behavior	Self-judged IT proficiency was in line with secure decisions; greater impulse issues are more likely to make poorer security decisions	Covariates Regression	67
Kajzer et al. (2014)	Investigate effectiveness of various InfoSec awareness messages upon users according to their personalities	Their exploratory results suggest that practitioners can be assisted in finding a more suitable way to tailor security awareness messages according to users' personality profiles.	Regression	293
Schuessler and Hite (2014)	Explore the relationship between several factors (e.g., personality and work ethics) and the strength of password chosen by users.	The user's password strength were related with their personality and work ethic	t-test, 2-tailed, and 1-tailed	71
Shropshire et al. (2015)	Investigate the impact of personality upon user's security software usage	Agreeableness and conscientiousness have strong relation with whether users would use security software	A components-based structural equation modeling	170
Johnston et al. (2016)	Study the impact of dispositional and situational factors upon violations on InfoSec policy	Their results suggest that the connection between situational factors and security policy violation can be moderated by using dispositional factors	A generalized form of the standard linear model	242

Table 4.1: Existing work on investigating the relationship between various demographic and personality factors and user's security behavior

4.3 Methodology

Motivated by the prior literature, this survey was designed to investigate the extent in which users are making risk informed decisions and the risk level associated to each user's activity. As this information security behavior is influenced by a number of factors, this survey is sought to explore the role of variations in demographics, IT background, level of online activity in terms of the frequency of using online services and personality traits, i.e. user-centric factors, on users' risk exposure and in shaping their risk informed behavior. From this point, the term user-centric factors will be used, in all cases unless otherwise specified, to refer to user's characteristics. The terms user(s) and end-user(s) are used interchangeably. Whilst the term security behavior is utilized throughout this thesis, in all cases unless otherwise specified, this refers to behavioral intent rather than actual behavior. Accordingly, this survey, as illustrated in Figure 4.1 , seeks to:

1- Get an overview of participants ' demographic characteristics such as age group, gender, education and personality through the Big Five Inventory personality traits (BFI).
2- Investigate whether users use different Internet-enabled devices
3- Measure the risk exposure, appetite, of users
4- Explore if the nature of risk changes associated to variations in certain user-centric factors such as demographics and level of online service usage.
5- Understand the relationship between risk posture and user-centric factors.
6- Assess the risk behavior of users according to the following:
    a. *Password hygiene*, i.e. frequency of changing passwords, password sharing, password strength and how to keep track of passwords.
    b. *Public access networks* , i.e. the frequency of use.
    c. *Social networks*, i.e. the frequency of engaging in social networks, accepting invitations and type of information shared.

d. *Security measures*, i.e. what security measures are used, how frequently they update their security software, what problems they have with security measures and how they respond to security warning messages

e. *Security breaches*, i.e. the kind of losses due to a security breach and to whom they reported it.

f. *Precautions taken* in the case of downloading email attachments whether from a known or an unknown sender, the use of USB drives and encryption and locking of their devices.

Therefore, the following research questions (RQ) were created:

RQ1: "*What is the general risk level associated with a user's security behavior*?"

RQ2: "*Is there a relationship between user's-centric factor X and the risk level of security behavior y*"

RQ3: "*If there is a relationship between user's-centric factor X and the risk level of security behavior y, how strong is that relationship*"

Since this survey is targeting users from the general public and in order to maximize the number of participants across a broad spectrum of backgrounds and IT levels, it was decided to use a quantitative method to collect data. A quantitative-oriented survey will enable generic statistical models (e.g., Pearson's correlation) to be applied on the response. Over long distances, an online questionnaire is particularly effective in gathering data from as large as a population sample of the general public as possible in a short time. Moreover, it was decided that questionnaire questions to be objective and achieve the aims of the survey. In order to be understandable by the general public, questions should be jargon free.

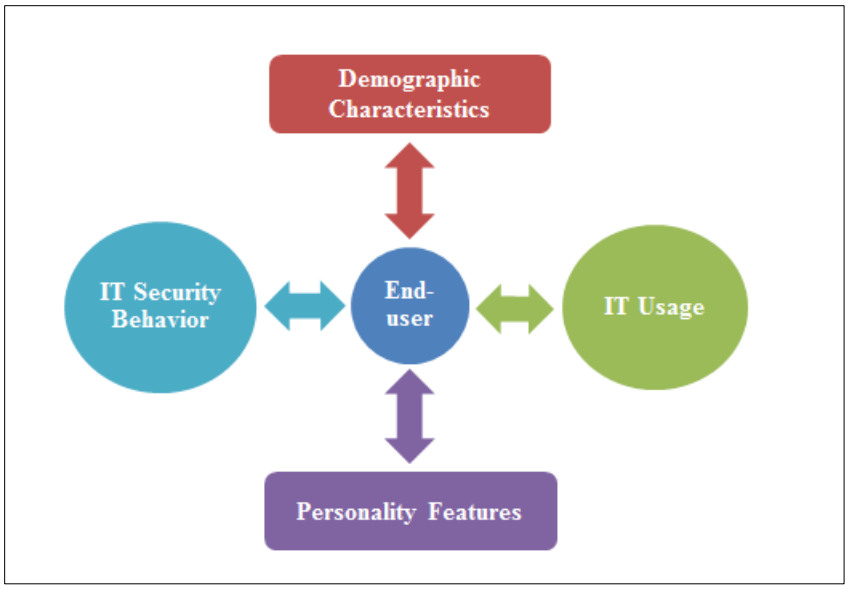

Figure 4.1: Survey's Methodology

During the preparation for this survey, an ongoing project at the Center for Security, Communication and Network Research (CSCAN) at University of Plymouth, Clarke et. al (2016) produced a questionnaire that contained elements the researcher needed to evaluate. Furthermore, it answered the fundamental question about risk and personality and its questions met the criteria set by the researcher. As this survey is part of the evidence gathering about the proposed PhD topic and (Clarke et. al 2016) was done by the same research group as the researcher, it was advised to use the data set already collected and perform an independent analysis from this perspective.

However, the dataset suffered from a skew towards IT background (65%). In order to get rid of this skew and make the population sample more representative of the general public with users varying IT levels from novice to technology savvy, it was decided to redistribute the online questionnaire targeting non-IT professionals in particular. To ensure a high response rate, the researcher distributed the link to the online survey to a wide range of people but with the condition that they are 18 years or older and neither an IT professional nor an IT student. The link was promoted via email, popular social networks such as Facebook and Twitter and instant messenger such as WhatsApp. In total, 563 completed responses are gathered. However, 538 participants'

responses are selected for the analysis as the other 25 participants answered wrongly to at least one of controlled questions and their responses are removed completely from the study.–The data collection stopped when the IT proficiency skew changed from 35% of non-IT professionals to 53%.

To analyze the security behavior of users and how it is influenced by variations in age, gender, IT proficiency, IT service usage and personality traits, three levels of risk, high, medium and low, were associated to each participant's behavior. The traffic light terminology was used in which red represented high risk level, orange for medium and green for low risk level. Further to that, three steps of analysis were performed as follows:

Step 1: To measure the risk exposure of users, the behavior of the population sample in general was analyzed according to aspects in Figure 4.2.

***Step 2*:** Users are, first, categorized according to age, gender, IT proficiency, online service usage and personality trait as illustrated in Figure 4.2. As for each personality trait, for example, participants are classified as either high (+) in a trait, i.e. the average BFI score is greater than 3, or low (-), i.e. the average BFI score less than or equal 3. Second, their security behavior is analyzed according to aspects of Figure 4.2. However, this is done to explore the effect of each of these factors on user's behavior risk level and if it changes accordingly.

A null hypothesis was generated as " *There is no relation between variations in user-centric factor X and the risk level of security behavior Y*"

Where *X:* Represents the studied user-centric factors of IT proficiency, Age, Gender, online service usage and personality traits. *Y:* Represents the assessed security behaviors, i.e. 33 security behaviors. Pearson Chi-Squared Test was used to determine the significance effect of variations in each studied factor on users security behavior. The p-value is calculated for each factor/security behavior so that if it is less than a pre-

determined threshold , i.e. 0.05, then the relation is statistically significant and the null hypothesis is rejected, otherwise not.

Step 3: Similar to level 2, users are first categorized according to their user-centric factors as illustrated in Figure 4.2. Second, to determine the correlation between user-centric factors and each security behavior, the survey data is examined using the Bi-variate Pearson two-tailed correlation according to aspects as shown in Figure 4.2.

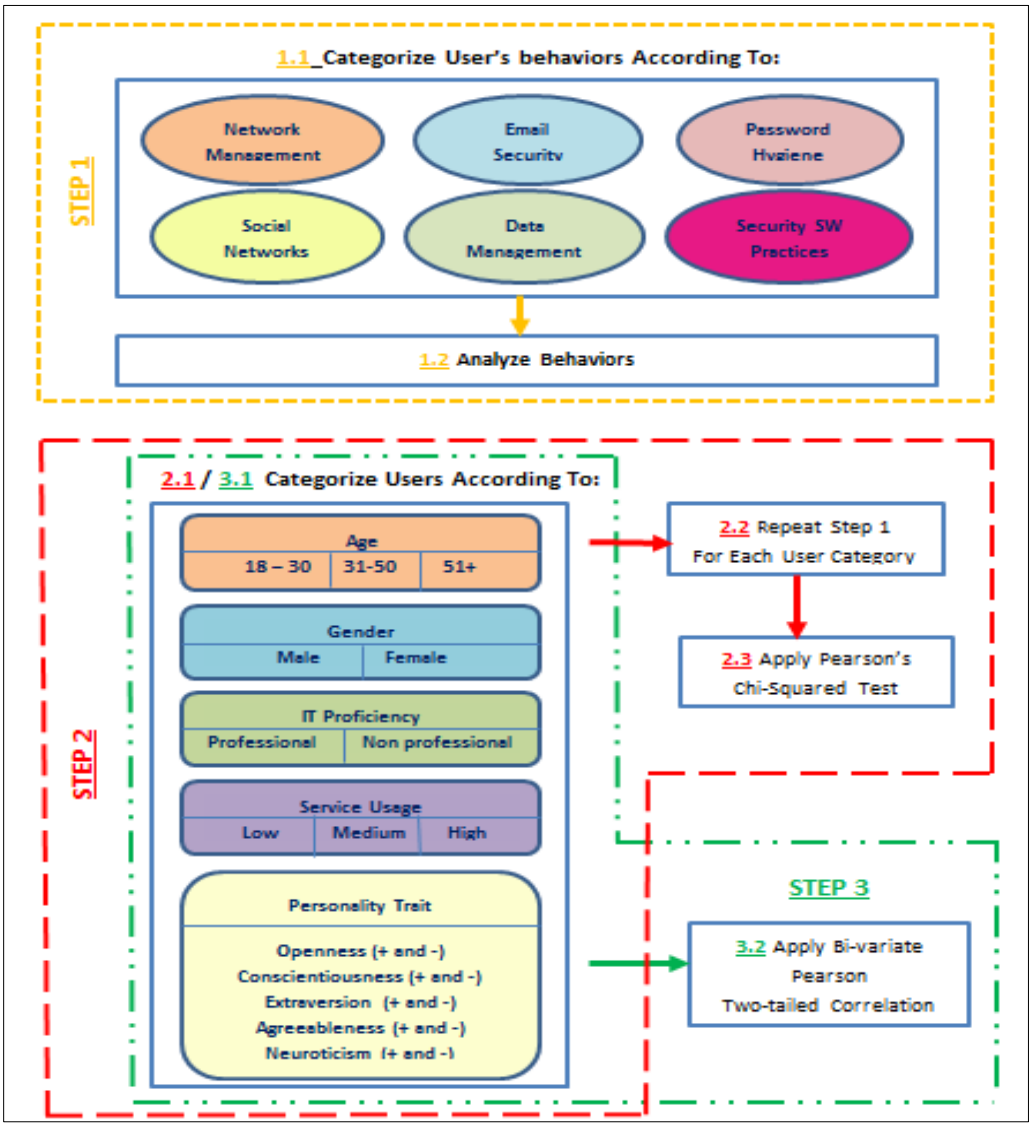

Figure 4.2: Analysis Framework

4.4 Survey Findings

An analysis of the demographic characteristics shows that more than 71% of participants are males and 62% are in the age group from 18 to 30. A fairly even split was found in the IT background of participants where 53% were found to be non-IT professionals. In addition to the fact that the majority of participants (71%) are students, 68% of them had at least an undergraduate level of education. This could be because of the author's personal contacts. Moreover, 67% of participants reside in Europe as shown in Figure 4.3.

Although the analysis results of this survey are likely to be skewed towards age and gender, but the population sample presents a relative representation of technology users. To this end, it is in-line with the United Kingdom's Office of National Statistics findings that the age group (16-34), regardless of gender differences, where found to be the top users of Internet services (Ons.gov.uk 2013). Further to that, it could be suggested that they are more likely to be IT literate which allows them to provide a more educated and informed response to the surveyed questions.

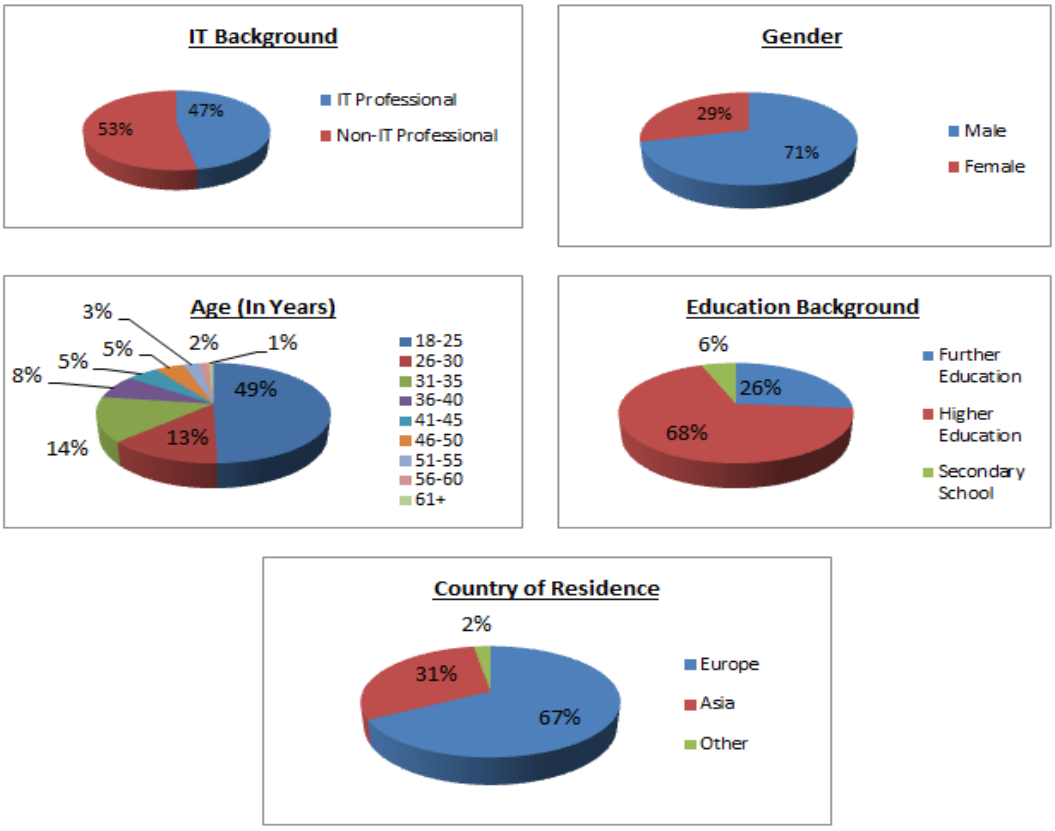

Figure 4.3: Summary of Participants Background Information

In order to analyze participants technology use and services, they were asked about the digital devices they use. Unsurprisingly, as illustrated in Figure 4.4, participants own an increasing number of devices where 76% of them have at least 3 digital devices from various manufacturers and represent a variety of models and sizes.

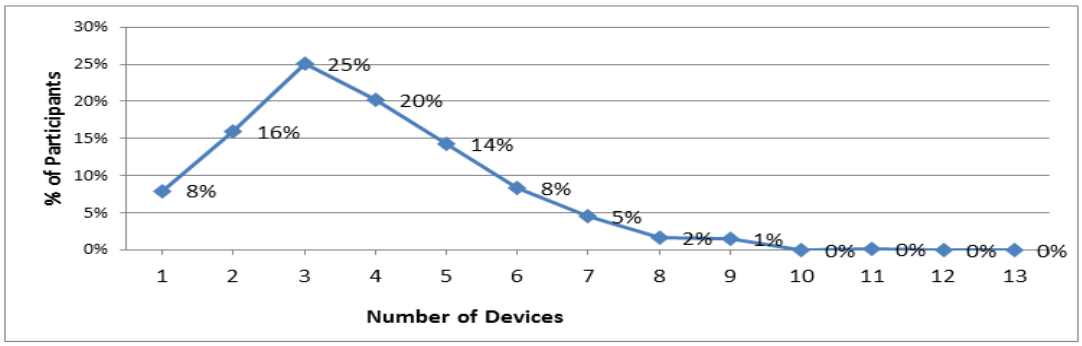

Figure 4.4: Number of Owned Devices

Moreover, devices used/owned ranged from desktop/laptop computers to tablets, smartphones, game consoles and smart watches as illustrated in Figure 4.5. Windows enabled desktop/laptop computers take precedence over its rivals, Mac and Linux by 81%. In terms of tablets/smartphones, Apple's iPad/iPad mini and iPhone tip the scales with 75% over its competitors Android 54%, Windows 10% and Blackberry 7%. However, this popularity of these three are consistent with market share analysis (Gartner.com 2015). Regarding other Internet enabled devices such as game consoles, navigation devices, smart TV's and smart watches, they were utilized by 37%, 29%, 24% and 4% respectively. This diversity of platforms and operating systems is challenging as it increases the knowledge burden on users in maintaining security of these different devices.

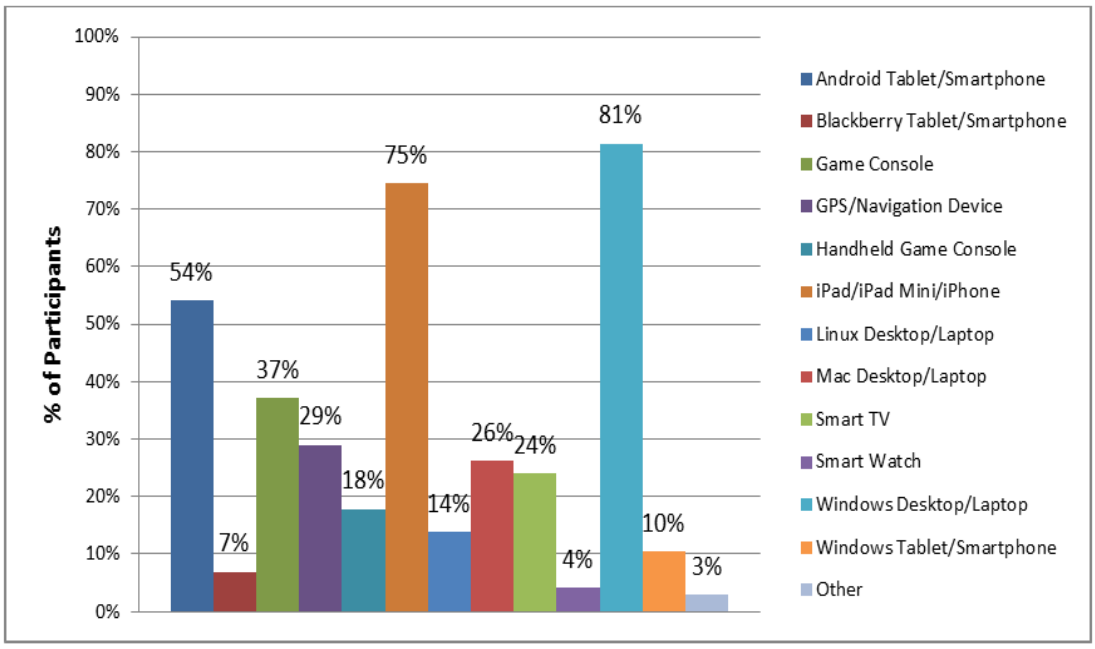

Figure 4.5: The Used Digital Devices

In addition to their device usage, participants' usages on online services were also examined. Based upon how frequently they use these services, three levels of usage are obtained: high (i.e., *always*), medium (i.e., *often*), and low (i.e., *sometimes, rarely and never*). As illustrated in Figure 4.6, email is the most popular service as 77% of the participants had a high usage; in addition,

office applications, instant messenger, online streaming, and social networking are also very popular as more than 70% of the participants claimed that they use these services on at least *often* basis. To this end, this popularity of email arguably increases participants' vulnerability to email related security threats such as phishing. Additionally, the popularity of other services such as instant messaging and social networking may suggest that they could be used as an attack vector by hackers. In contrast to these popular services, P2P was the least used service where almost 26% of participants used this service. Continuing the trend of analyzing concurrent use, 87% of surveyed have access to minimum 5 services at a high/medium basis, suggesting majority of the participants highly engage with different IT technology and services.

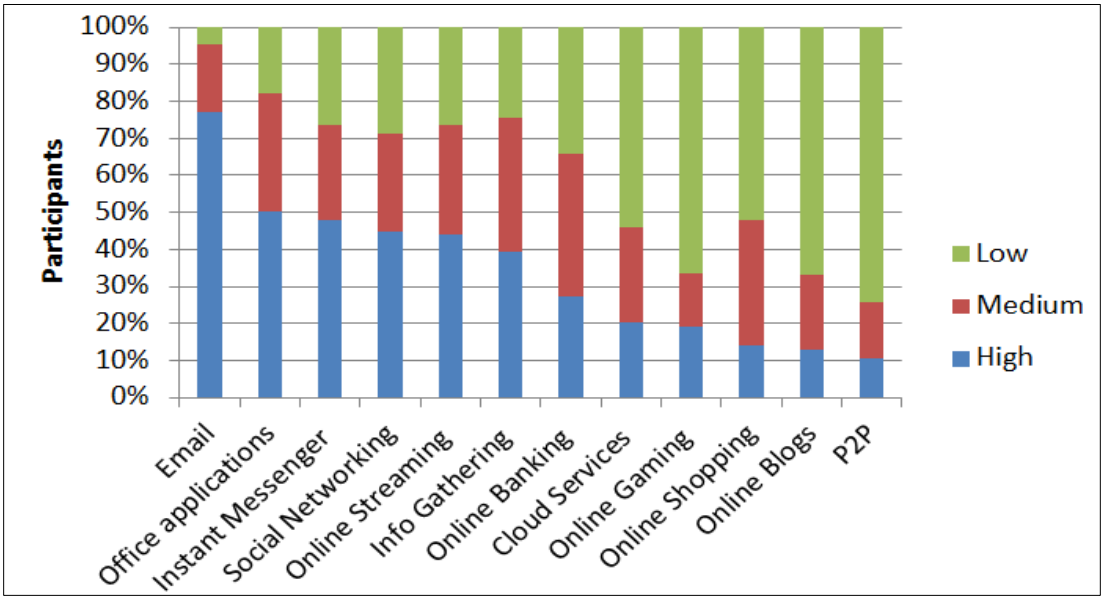

Figure 4.6: Usage of IT Services

The results of these two figures suggest that users are no longer relying on a single device and access services from a number of different operating systems and platforms. Hence, increasing the risk level of users where attackers have a wider range of attack vectors across a range of platforms. This places an ever increasing burden upon users to be aware of the risks and how to well protect themselves.

In spite of this high access and reliance on various services, an obvious question to ask is about the used security measures as one of the lines of defense against security attacks. To identify participants who might have provided arbitrary responses or exaggerated their knowledge, a fake security measure, '*Intrusion Attacking System*', was included in the list of security measures and a couple of fake terms, '*Whooping and Phibbing'*, in the list of security incidents. However, a relatively small number of participants (4%) selected these terms. This said, it is of little concern that these terms received any attention at all. Nevertheless, their entire entries were excluded. It was found that 4 different security measures at maximum were used by 22% of participants as depicted in Figure 4.7.

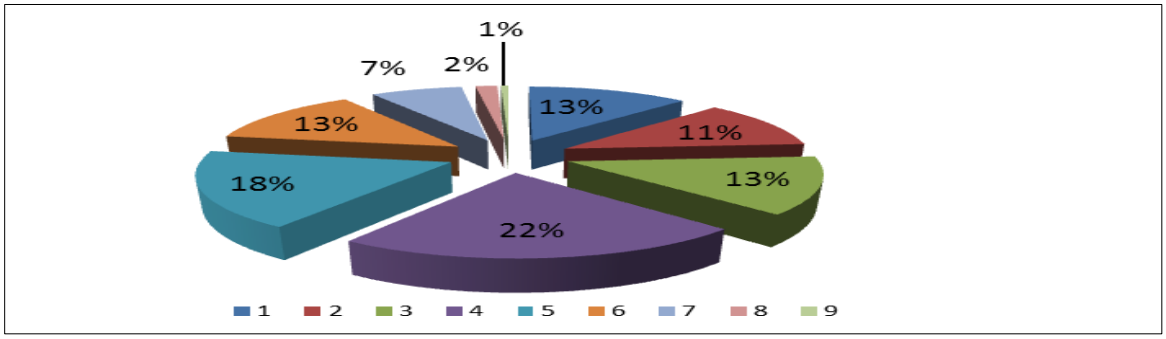

Figure 4.7: The Number of Used Security Measures

Figure 4.8 reveals the popularity of Anti-Virus software as a security countermeasure where it was utilized by 88% of participants followed by secret knowledge in 69%. However, firewalls and data backup were used by almost two thirds of surveyed users.

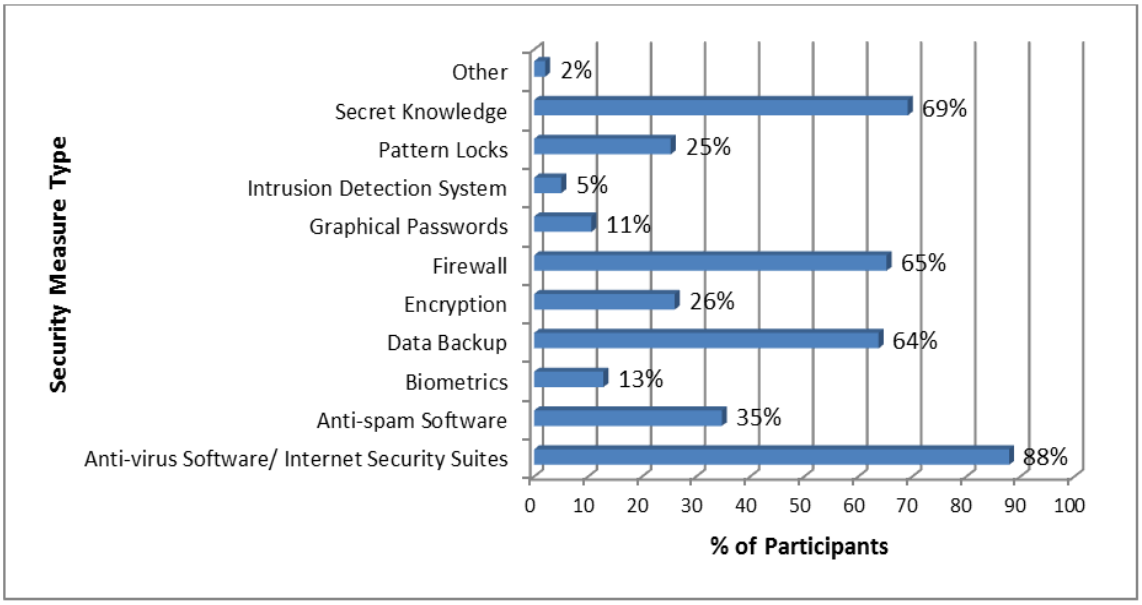

Figure 4.8: Types of Used Security Measures

To estimate the level of risk associated with their security practice, participants are initially asked how often they perform an activity, i.e., *always*, *often*, *sometimes*, *rarely*, and *never*; which were then codified into three risk levels (i.e., high, medium, and low) based upon the types (i.e., positive and negative) of the security activity. For the positive security activity (e.g., a user scans a USB drive before using it), the more frequent the user performs it, the lower the risk level is associated to it. Therefore, for the positive security activities, "*always*" is coded into low; "*often*" is coded into medium; and "*sometimes*, *rarely* and *never*" are coded into high. In comparison, for the negative security activity (e.g., a user stores his/her passwords), the more frequent the user does it, the higher the risk level is linked to it. As a result, "*always*, *often*, and *sometimes*" are coded into high; "*rarely*" is coded into medium; and "*never*" is coded into low for the negative security activities. Thus, participants behavior was analyzed according to various aspects as follows:

4.4.1 Password Hygiene

Many techniques and tools are used by hackers for cracking or guessing passwords. Moreover, cracking passwords is easier if they are weak or short or contain personal information such as

birthdate or names. A hacker can easily gain entry to a system by hitting on a password through a dictionary search, for example. Hence, one way of protecting information from theft or unauthorized access is to use a strong password. A password that contains a mixture of upper and lower case letters, numbers and special characters and is more than eight characters in length is a difficult to crack password (Alarifi et al. 2012).

As a result, it is important that users use their passwords in a secure manner. Participants appreciate the need for passwords as means of protection as almost two thirds of them always use one to log into their home computers. However, a surprising result was that 81% of participants failed to apply strong password requirements on 81-100% of their passwords. Despite the use of a strong password is effective to protect systems from password cracking, participants are in high risk of password cracking attacks as more than four fifths of the participants' passwords were poorly created.

However, choosing a strong password is not enough to ensure the security of information and offer the required level of protection as passwords need to be changed on a regular basis. A great lack of secure behavior was found among participants as only 6% of them changed their passwords in less than three months. Also, less than two thirds of the participants change their passwords regularly (i.e., within a 6-month timeframe); and 42.2% of the participants only change their passwords if they were asked (e.g., a system may force its users to change their password every 6 months), providing a large window of opportunity for attackers if a user's password is compromised. Hence, having a weak password that is not changed frequently is a major security risk.

Nevertheless, 46.3% of participants have less than 6 passwords for all their services and devices, providing a strong indication of password reuse as 98.1% of the surveyed use 10 services and/or devices or more. This is reiterated by finding that merely 20% of participants never use the

same password for multiple sensitive services. This offers opportunities to attackers who can obtain access to multiple systems by only successfully hacking into one of the systems. Hence, this high risk level behavior suggest that participants are facing hard time in remembering different passwords for various services.

To keep track of their passwords, data collected suggests that participants are in favor of storing their passwords such as writing it on a post-it note or by using password stores. This is evident as almost two thirds of participants store their passwords. Another way for remembering passwords could be by allowing web browsers, systems or applications to remember them. Unfortunately, 80% of participants are in favor of this high risk practice. One possible way to reduce the vulnerability of an attacker steeling session information and cookies from tracking user's online activities is to log off from these online services when done. This need is increased when accessing sensitive services such as banking and Government. However, only one quarter of the participants practice it safely by logging off from online systems activities when done. It is envisaged that both activities offer some levels of user convenience (e.g., saving time) and users have less concerns as these browsers/online systems are initially protected by the main OS authentication mechanism (assuming it is correctly used). In contrast, participants appreciate the role of the password for workstations as more than two thirds of them lock their stations when they are away from desks.

The best password hygiene practice employed by participants in general was that in them never sharing passwords with others. This was prevalent as almost 62% of participants have low risk as they never share their passwords with others. A similar result is presented in Helkala and Bakas (2013) that 63% of their 1,003 users do not share their passwords. Unfortunately, the results also highlight that almost two fifths of users have experience of sharing their passwords, demonstrating

that an opportunity exists for a high level of misuse on IT systems and data as illustrated in Figure 4.9.

Based upon these results, it shows that significant effort is required on reducing the risk of password practices even for users with a more technical savvy and educated background. Password practice activities that are associated with high risk levels are also linked to user convenience: system security is compromised as user convenience is more preferred. Therefore, additional consideration regarding usability and security should be given by designers when developing new systems.

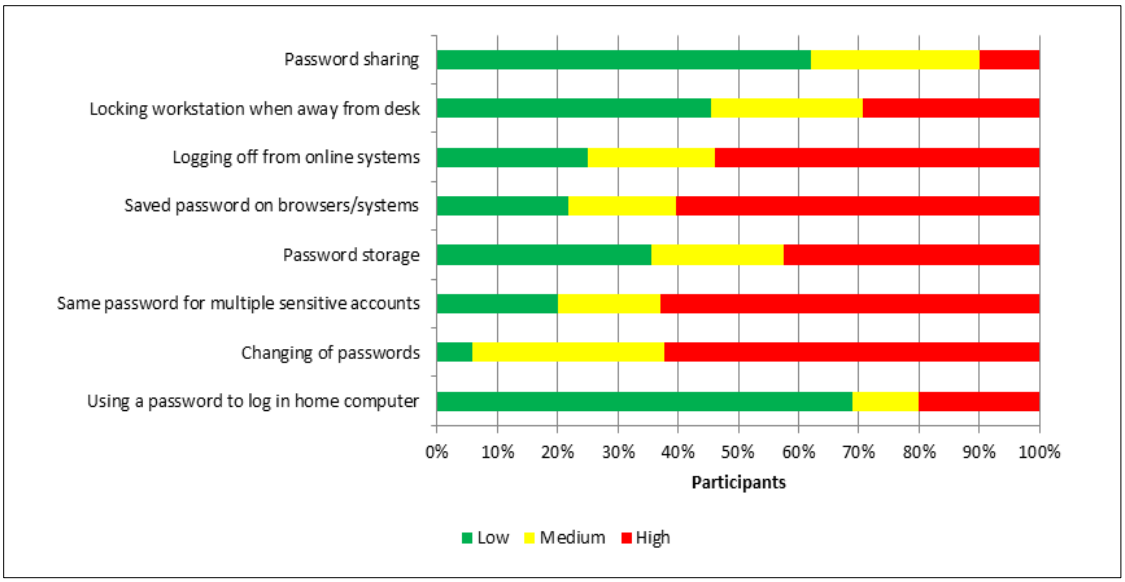

Figure 4.9: The Risk Level of User Password Hygiene Practices

4.4.2 Social Networks

One of the popular Internet services is social networking where almost 2 billion users around the world use social networks such as Facebook and google+ in 2015 which is expected to rise half a billion in 2018 (Statista.com 2016). This popularity was reflected in the surveyed users as only 5% of them never engage in social networking. Nevertheless, social networks are used as a common threat vector by hackers to collect information about people that is used in identity fraud (Talib et al. 2010). However, this highly depends on the kind of activities performed by social

networkers. Unfortunately, the risks of sharing information online are underestimated by users and tend to mistakenly choose their privacy settings in favor for social networks benefits that may result in unintended parties sharing information with them. This may result in an increase in privacy and security threats (Bachrach et al. 2012; Halevi et al. 2013; Egelman and Peer 2015 a and b). This informed behavior is lacking when it comes to the type of information shared online. However, as illustrated in Figure 4.10, amongst all participants, a common high awareness level is shared by more than half of them as they never accept invitations from people unknown to them which demonstrates a more careful and informed behavior.

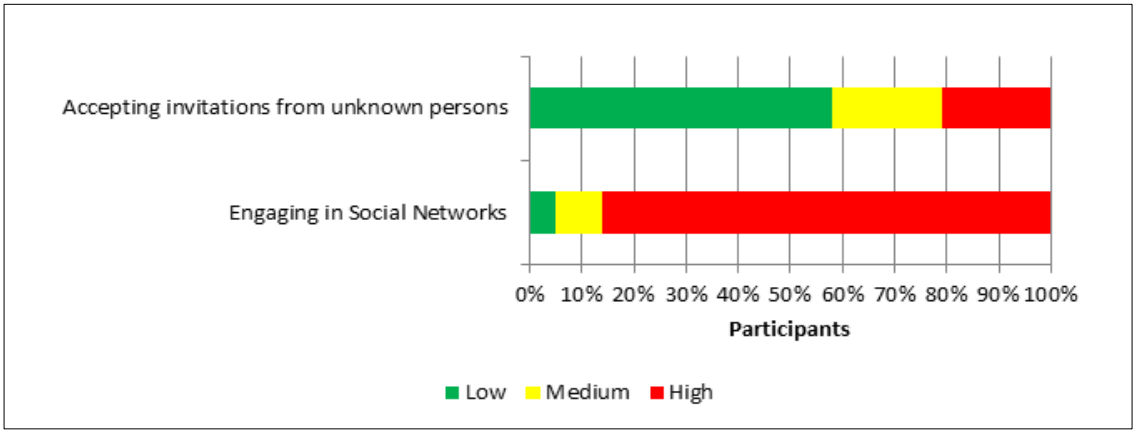

Figure 4.10: The Risk Level of User Social Networks Practices

4.4.3 Security Software Practices

Although the utilization of security measures is a step towards protection against security incidents, but this is not enough. The idea is in how these security measures are maintained by the user. Four fifths of participants experienced non-physical security incidents such as data loss, phishing and malware compared to almost half of them (56%) experienced physical security incidents such as device loss and hardware failure. To this end, the survey moves forward to assessing participants' security software behavior.

One common security practice is to update systems/applications regularly as a range of vulnerabilities could exist in unpatched software. As basic security measures such as Anti-Virus

software and Firewalls were implemented by the majority of participants as in Figure 4.8, the question was how frequently they were updated to cope with the regularly introduced malware.

Although more than half (52%) of participants always update their Anti-Virus software as illustrated in Figure 4.11, the other half of participants put their IT systems into a more risky environment as an adequate level of protection cannot be provided by antivirus software with out-of-date signatures. Indeed, Microsoft's biannual Security Intelligence Report suggests that the infection rate of Windows OSs with out-of-date security software is more than three times higher than those with latest signatures (Microsoft.com 2014).

What if the user's computer performance slowed down, because of the installed Anti-Virus software or Firewall? How users are going to behave? Are they annoyed and going to simply disable them or not? Fortunately, more than half (59%) of surveyed users were knowledgeable of the consequences of such behavior and never practiced it. As a result, low risk level was prevalent among participants.

By further generalizing the assessment of user's behavior to include all installed software in terms of installing the latest updates and security patches and if they canceled or postponed a security related update when notified to do so, the findings were intimidating. Almost one third of participants in general '*always'* install patches and '*never'* cancel security related updates endangering their systems, with 85% of exploitation attacks related to unpatched software, i.e. posing medium to high risks to their systems, (Canadian Cyber Incident Response Centre 2015). With the continuously evolving threat landscape, the importance of patches as a methodology for fixing vulnerabilities in pre-installed systems that may be exploited by malware is paramount.

Interestingly, a comparison of these results highlights a similar pattern that is obtained from the password practice in terms of user convenience. Regarding Anti-Virus Software update, the burden

upon the end-user is removed or at least reduced as the process is typically configured as automated. Conversely, the end-user's attention is more required for patching: either to approve it or to wait whilst an automated patch is installed, and often more inconveniently a reboot of the system could be required. Nevertheless, knowing that technology alone will not provide the required level of protection, this highlights an interesting fact that whenever the user is involved in the security process as in updating the software the burden is increased on him. This suggests the need for an automation of these tasks or at least in better communicating the risks to the user in a user-centric persuasive manner to convince him of changing his behavior.

With the growing prices of software, it may be cheaper or free to install or use pirate software. This illegitimate software when installed, may contain spyware that can exploit user's data such as passwords and credit card numbers by identity thieves. Further to that, vulnerability to various attacks are increased as these counterfeit software are unable to incorporate updates released by vendors. Surprisingly, such behavior was experienced in almost two thirds of surveyed users posing high risks to their systems. Further analysis reveals that a quarter of the total participants perform both activities of disabling Anti-virus/Firewall and the utilization of pirate software ; yet 72% of them claimed that they are experienced and expert IT users. This phenomenon could suggest that while technical users understand better security they may also be the ones who put the IT systems at a higher risk.

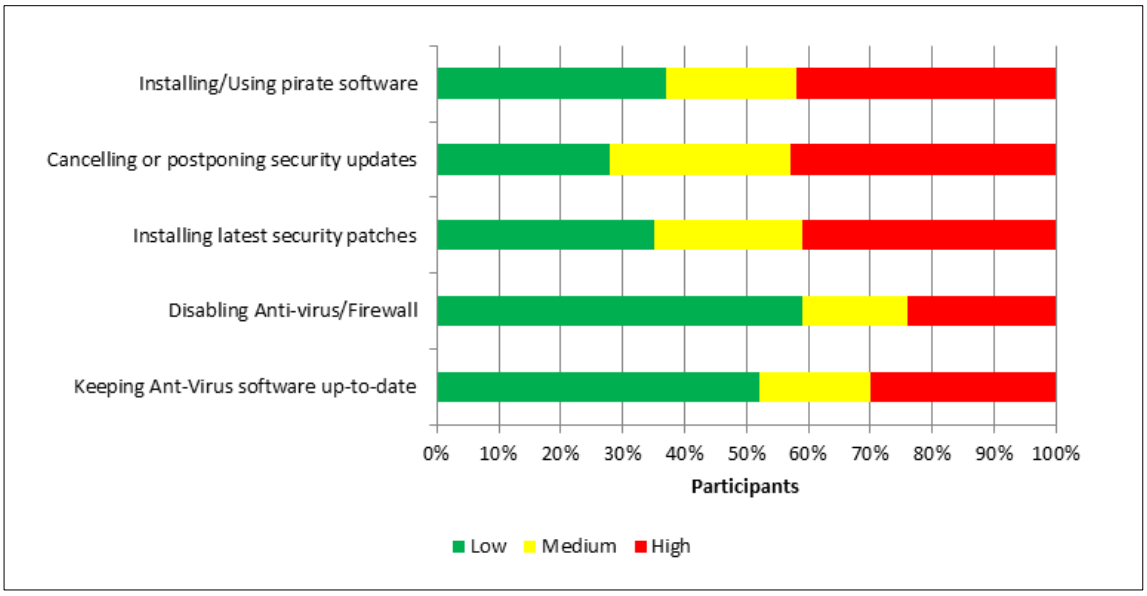

Figure 4.11: The Risk Level of User Security Software Practices

4.4.4 Email Security

With the high popularity of email service, where 96% of participants use it on an '*always/often'* basis, rises the threat of email related incidents such as phishing, spoofing and spam (Kaspersky 2017). Phishing attacks are getting more sophisticated and targeted (spear phishing) in an attempt to make fraudulent emails look like legitimate emails and enhance the attacks response rate. The aim of these attacks is to convince users to reveal their personal information and use it to impersonate the user. Hence, participants susceptibility to fall victims to such attacks were explored. A fairly good behavior was demonstrated as almost two thirds of the surveyed users never click on attachments/links in emails from unknown sources. In contrast, a strikingly converse behavior was practiced if the email was sent from a colleague or a friend. Almost 72% of surveyed participants seemed to be not suspicious of emails received from people known to them and tend be at risk as they open links/attachments in them without checking. This highlights the importance of trust and also potential danger when the sender's email was perpetrated. Nevertheless, this trusting behavior among participants suggest a lacking knowledge of spoofing attacks.

Spam, in which chain emails are a form of, is also an increasing threat to email users (Kaspersky 2017). The majority of participants were knowledgeable of such emails. This is evident as almost 78% never forwarded these emails. Subsequent good actions to receiving such suspicious emails is to always delete them and notify IT support. However, two contradicting behaviors were observed. On the one hand, participants' behavior is good in general as three quarters of the surveyed claim to delete them. On the other hand, low awareness of adequate behavior in notifying IT support was noticed. As illustrated in Figure 4.12, almost three quarters of surveyed users do *not always* report these tricky emails to IT support. Although such warning could benefit other users from being victimized, this could be due to several reasons such as participants feeling ashamed to report such incidents, do not know whom to report it to or simply think that this is of no interest to others. Nevertheless, this practice could reduce the speed in dealing with threats.

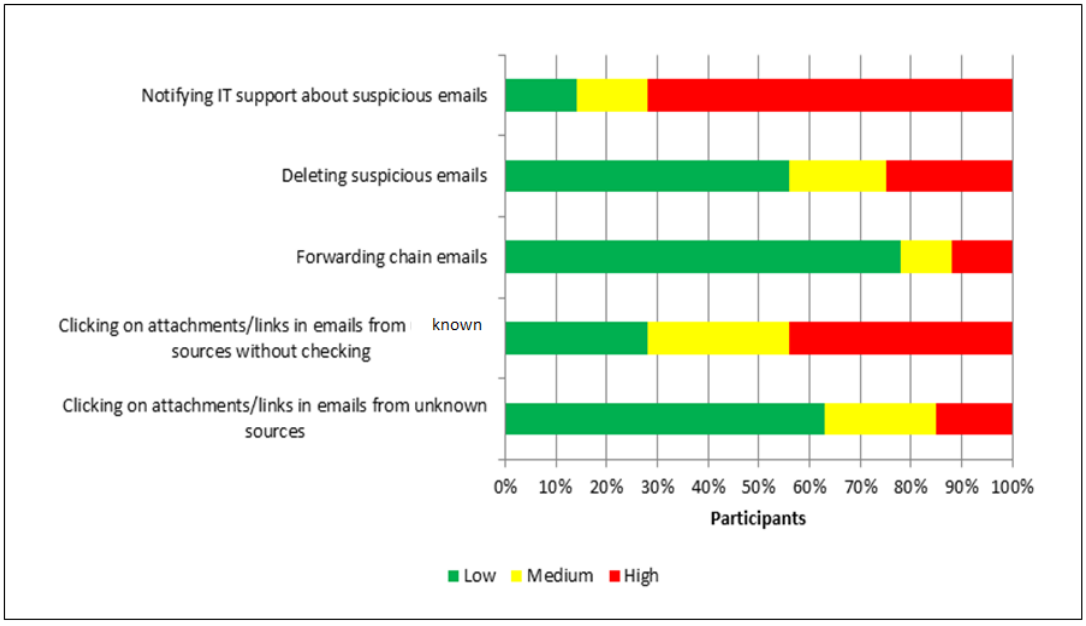

Figure 4.12: The Risk Level of User email Security Practices

4.4.5 Data Management

Today, users are more connected to their computing devices and rely on them in their everyday lives such as chatting with friends, finding the nearest restaurant and as means for storing data.

Moreover, users are storing various types of data such as photos, contacts and health information on their computing devices. Hence, the risk of losing such data may have a devastating effect. Therefore, an obvious and easy solution is to backup this data on a regular basis, regardless of the used digital medium, to restore it whenever needed. Moreover, being aware of most common risks that may jeopardize the confidentiality, integrity and availability (CIA) of data, encryption could be used as an enabler to achieve an acceptable level of data security and privacy. To this end, combining these two good practices will provide confidence that user's data is safe even if this backup is stolen.

Across most of the surveyed users, a disturbing finding was that they fell short of practicing good behavior in both backing up their data and encrypting it. Regardless of the popularity of data backup as a security measure, almost two thirds of participants as in Figure 4.8, less than one third of participants are in low risk as they always back up their data on a regular basis as demonstrated in Figure 4.13. However, this suggests that participants do use this service but with lower frequency than expected.

A USB drive is a cheap and easy to use medium for storing and transferring data between computers. With this, comes a greater chance of them being stolen, lost or used to spread malware such as viruses. Therefore, a good practice is to always scan such drive before using it. The most terrifying statistic is the prevalent insecure behavior among participants. As only 15% of participants '*always'* scan a USB drive before using it. However, a contradicting trend was found when it comes to inserting and accessing USB sticks from unknown sources where 40% of surveyed users '*never'* practiced such behavior.

Unfortunately, encryption seemed not to be a popular practice by surveyed users. This is apparent as only 7% of participants *always* use encryption when transferring data via a USB drive

and 12% claimed they always encrypt sensitive information that is stored on their computer. This suggests the need for further education on the benefits of encryption and how to practice it.

In the case of hardware disposal, a good preceding practice to protect security and privacy is to always destroy all data stored on it. Luckily, a high level of awareness was found among participants as two thirds of them regularly destroy their data before disposing of hardware.

In order to protect their IT system from various attacks, end-users should practice better security on data, such as paying more attention to security warnings. More than four fifths of the participants open a document despite security warnings as demonstrated in Figure 4.13. This suggests that security software is failing in effectively communicating the risks to users and convincing them of the consequences that may occur in case they disobey such warnings.

The last data management behavior that was assessed was the decision to download files from suspicious websites or not, as they may be packed with malware and spyware. However, a noted informed behavior was remarkable as almost one third of participants never trust these websites. Nevertheless, extra education and awareness raising of the threats of such "not safe" files are required for those who undertake such behavior.

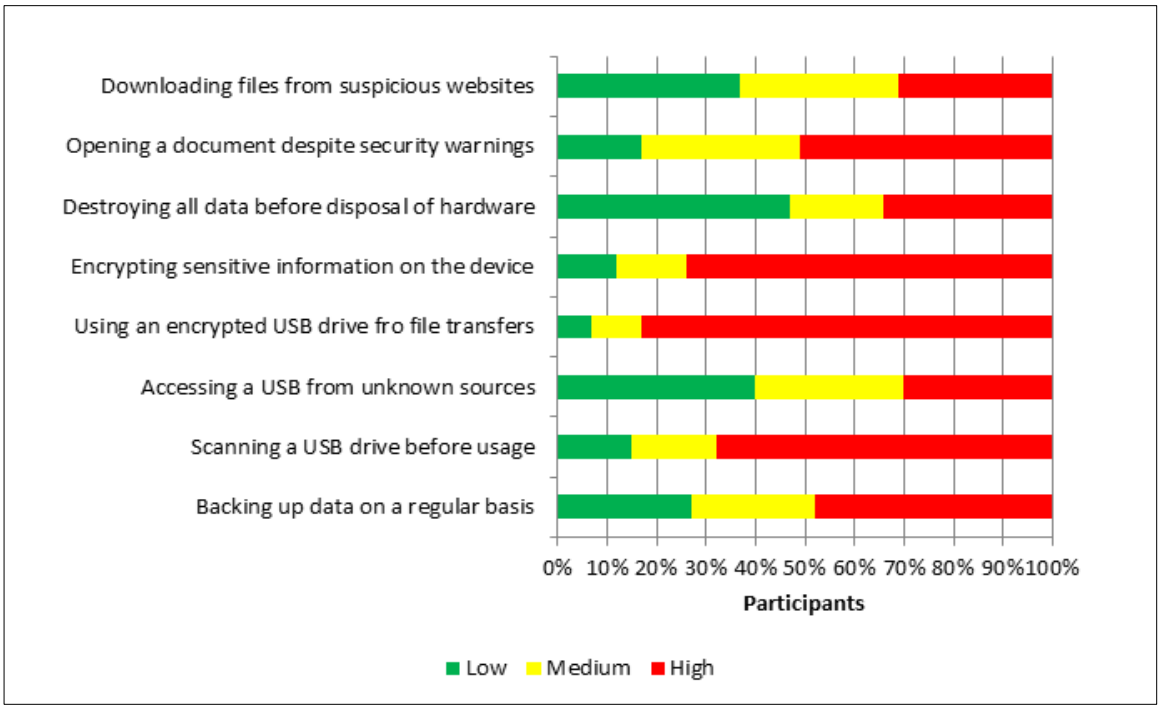

Figure 4.13: The Risk Level of User Data Management Practices

4.4.6 Network Management

Good network management is essential to protect devices and its data against various network related attacks (e.g. browser attacks and man-in-the-middle attack). It is common practice that network security managers and IT administrators are responsible for securing business networks and servers. However, it is mainly individual's responsibility to protect their own endpoints.

However, users do have more control over the use of wireless technology on their devices. Users can be online by simply connecting to a public WiFi network that are almost found everywhere from shopping malls to coffee shops free of charge. This allows the exchange of data between the user's device and access point in clear air, unencrypted. As a result, any exchanged communication can be easily eavesdropped by an attacker. Hence, connecting to such networks is not as risky as the kind of activities performed when connected to these networks such as accessing an online banking account. To assess user's vulnerability to such threats, the survey proceeded by asking participants about the frequency of using public access WiFi networks. A common finding,

as shown in Figure 4.14, is the great lack of awareness in wireless network threats among participants exposing them to a high risk level. This is evident as only as low as 8% of participants never connect to public WiFi networks suggesting the need for further awareness/education.

Another good security and privacy maintaining practice is to always disable unnecessary wireless technologies such as WiFi and Bluetooth when not using them. Hence, the more services running on a computing device the more the chances for attackers to use them as a threat vector by breaking into or taking control of the computing device through them. However, a disturbing insecure behavior was practiced by participants as more than three quarters (81%) do *not always* disable wireless services when not used. This could be a result of either them not being aware of risks related to such practices or due to their heavy reliance on them that they want to easily and rapidly access them.

The use of an anonymizing proxy or the TOR network is a for (from user's point of view) and against (from system administrator's standing point) area in terms of security and privacy. Nevertheless, the survey result shows that less than one third of the participants *always* use the technique for anonymous communication. A Virtual Private Network (VPN) enables end-users to connect to a private network and access information over public networks securely. Figure 4.14 shows that less than 5% of the participants utilize the service on an 'always' basis (i.e. low risk level). This could be because VPN technology is mainly used to access corporate networks and the participants were largely recruited within academic environment that is less business focused.

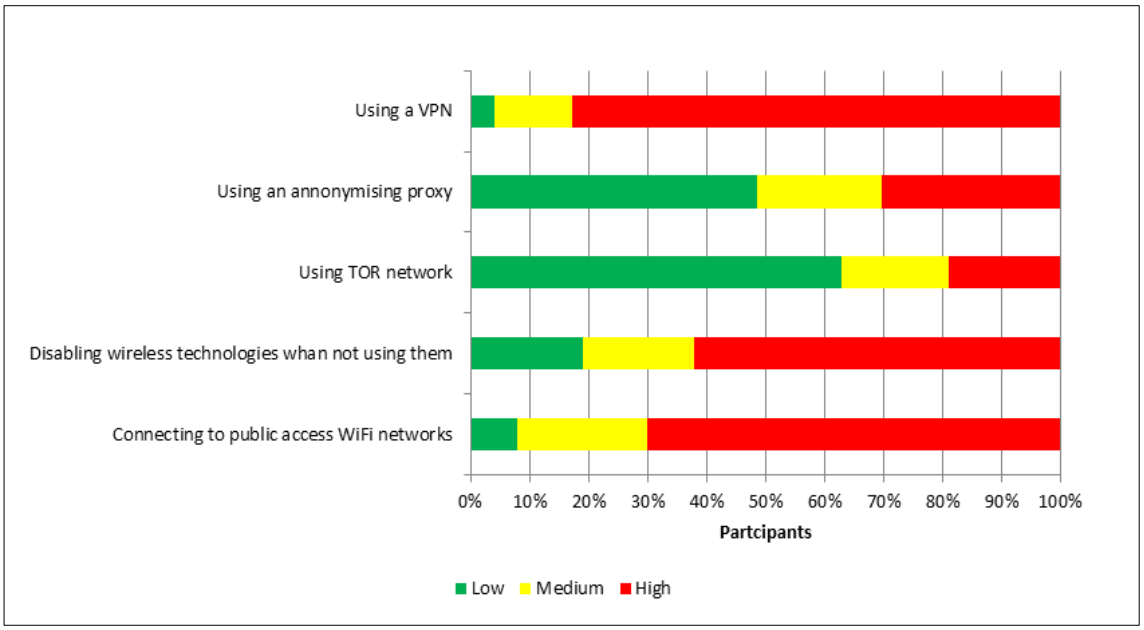

Figure 4.14: The Risk Level of Network Management Practices

4.5 Correlation Testing on The Relationship Between User-centric Factors and The Risk Taking Behavior

To determine the significance effect of the studied user-centric factors on the risk level of each surveyed intended user behavior, two statistical tests were used as explained in Section 4.3. Pearson's Chi-square test was used first to determine the significance effect of the studied factors on each user's behavior risk level. Then, the Bi-variate Pearson two-tailed correlation was used to explore the relationship between various user-centric factors and the risk level of user's intended security behaviors. For the purposes of clarity and because the second test included both correlation and significance, the output of the first test is as in Appendix A. The correlation output of the risk level of survey security behaviors and 5 user-centric factors (including personalities) is presented in Table 4.2. However, none of the user-centric factors were found correlated with 6 out of 33 surveyed behaviors, hence not included.

As shown in Table 4.2, amongst the personality factors, conscientiousness personality trait is negatively correlated with the risk of most user security behaviors (18 out of 27 are highly

significant (i.e., p-value of 0.01) and 3 are significant (i.e., p-value of 0.05)). This appears logical as people who score high on the conscientiousness BFI scale have been shown to be more responsible (Zhang 2006). A similar trend can also be observed from the agreeableness and openness personality traits; both are negatively correlated with the user's security behavior/risk level. The former and the latter are associated with 10 and 12 behaviors at a significant level respectively. In comparison, the neuroticism personality trait is positively correlated with the user's security behavioral risk level with 7 behaviors being statistically significant. This suggests people with high neuroticism are likely to be emotional more unstable; as a result, their security behavior might be more radical than others. With respect to extraversion personality trait, only one of the security behaviors correlated with significance. This suggests it is not a suitable moderator for predicting the risk level associated with user's security behavior.

Investigating the demographic factors, age is negatively related with the risk level of more than half of the end-user's security behaviors (i.e., 10 are highly significant and 6 are significant), suggesting the younger a user is, the higher the risk. One of the reasons behind this could be the more mature a person is, the more responsible they are. This is confirmed from a further analysis on the survey data that shows age and conscientiousness are positively correlated ($r=0.158^{**}$, $p=0.01$). Regarding gender, the results demonstrate little significance, with only the odd behavior flagging as significant.

Regarding the user-centric factors of IT proficiency and service usage, a general trend of negative correlation between end-user's security behavioral risk level and these factors is demonstrated by the results. The higher score of a factor, the lower the risk level associated to it. The results are almost self-explanatory: the higher the user's IT skill level and their familiarity with IT services, the lower the risk level is associated with their behaviors as they tend to understand more about IT services and would take IT security more seriously. Nonetheless, five positive

correlations (representing less than one third of total significant correlations) are presented between the service usage and the security behaviors, including Install/use of pirate software, Opening a document despite security warnings, and saved password on browsers/systems. The first two could suggest that users with a high level of understanding of IT tend to be more arrogant when dealing certain IT risks; while the last one could be caused by the amount of additional/repeated authentication that is often required for high usage users.

N=538	BFI					Demographics		Self-judged	
Security Behavior	E	A	C	N	O	Age	Gender	IT Proficiency	Service Usage
Password Sharing	*.091**	0.000	**-.163****	0.047	-0.074	-0.071	**-.181****	**-.168****	-0.046
Lock workstation when away from desk	-0.063	-0.031	**-.188****	-0.003	-0.069	*-.106**	0.031	**-.148****	**-.156****
Password storage	0.020	-0.070	0.009	-0.009	-.088*	0.0034	-.098*	**-.119****	-0.007
Log off from online systems	-0.052	-0.072	**-.182****	*.090**	**-.118****	*-.092**	-0.051	-0.060	0.070
Saved password on browsers/systems	0.013	-0.070	**-.173****	0.054	-0.005	**-.191****	0.035	0.051	**.238****
Same password for multiple sensitive accounts	0.037	0.030	**-.129****	*.096**	*-.092**	**-.220****	-0.056	**-.257****	0.046
Disable antivirus/firewall	-0.061	**-.112****	**-.212****	0.081	**-.116****	-.097*	-0.015	**-.209****	-0.063
Keep anti-virus software up-to-date	-0.013	-0.070	**-.222****	*.097**	*-.099**	*-.093**	*-.109**	**-.355****	**-.205****
Install security patches without any delay	-0.001	*-.101**	**-.176****	**.147****	**-.114****	-0.083	**-.206****	**-.278****	**-.229****
Install/use of pirate software	0.005	**-.123****	**-.159****	0.056	-0.050	**-.311****	**.174****	0.005	**.138****
Forward chain emails	0.034	**-.186****	**-.178****	0.082	**-.130****	-0.048	-0.012	**-.197****	**-.116****
Click on email links/attachments from unknown sources	-0.016	*-.098**	**-.159****	0.075	**-.128****	-0.001	**-.114****	**-.212****	**-.120****
Delete suspicious emails	-0.022	*-.095**	-.100*	0.057	*-.103**	**-.204****	0.059	**-.113****	-0.069
Click on email links/attachments from known sources without checking whether it looks suspicious	0.006	-0.063	*-.095**	0.042	-0.079	-0.009	**-.124****	**-.224****	*-.097**
Notify IT support about suspicious emails	-0.033	-0.024	-0.071	0.046	-0.041	**-.271****	0.080	0.000	-0.068
Destroy all data before hardware disposal	0.007	**-.116****	**-.141****	.094*	**-.150****	**-.124****	*-.095**	**-.231****	**-.161****
Accessing USB from unknown sources	0.005	-0.070	**-.132****	0.057	-0.035	-0.016	-0.033	**-.168****	-0.048
File downloading from suspicious/unknown websites	-0.034	**-.163****	**-.193****	**.114****	-0.057	**-.185****	0.047	-0.012	0.013
Performing regular data backup	-0.073	-0.054	**-.243****	0.072	-0.069	**-.188****	0.068	**-.212****	**-.165****
Opening a document despite security warnings	-0.016	**-.153****	**-.187****	0.061	-0.056	**-.262****	0.022	0.005	**.133****
Scanning a USB drive before usage	-0.046	-0.034	**-.145****	**.119****	**-.113****	-0.083	**-.128****	-0.062	**-.117****
Encryption for sensitive information stored on computer	-0.072	-0.046	-0.053	0.075	-0.068	-0.049	**-.113****	**-.137****	*-.111**
Use the TOR network	-0.059	*-.097**	-0.053	0.030	-0.01	*-.103**	**.138****	-0.004	0.055
Use an anonymising proxy	-0.071	-0.071	**-.133****	0.040	-0.023	**-.137****	**.232****	0.062	**.158****
Disable wireless technologies when not using them	0.008	-0.012	*-.096**	-0.017	-0.083	0.048	**-.134****	-0.072	-0.053
Connect to public access networks/Wi-Fi	0.051	-0.045	-0.028	0.038	-0.046	-.105*	-0.076	*-.091**	**.143****
Use a VPN	0.031	0.028	-0.028	-0.031	*-.104**	-0.076	-0.064	-0.082	**-.131****

Table 4.2: Pearson Correlation results on various user's factors and the risk level of their security behaviors

E: Extraversion; A: Agreeableness; C: Conscientiousness; N: Neuroticism; O: Openness;
* Correlation is significant at the 0.05 level (2-tailed), ** Correlation is significant at the 0.01 level (2-tailed)

4.6 Discussion

The results of this survey were obtained from a population sample that fairly represents technology users with different demographics, personality traits and varying levels of IT background. Although the population sample suffered from some skews in gender and age, but this does not affect the major results of the survey. Additionally, this survey was an opportunity to explore user's security behavior from a holistic view and how this behavior is affected by variations in IT proficiency, demographics (age, gender), IT service usage and BFI personality traits.

Apparently, participants interact with a wide variety of online services through a number of digital devices that utilize different platforms, varying security requirements and configurations. This implies the increased security knowledge burden on the user, especially that the majority of participants valued their need for information security as essential or high. Further to that, it was evident that even those with a good IT background failed to securely implement some basic security practices such as downloading files from suspicious websites and using the same password for multiple sensitive accounts.

With the continuously evolving threat landscape and users' augmented reliance on technology and services, the requirement of up-to-date security awareness is a must for users to remain secure. Moreover, the varying differences between users should be taken into account. Therefore, the necessity to continuously protect users' information on a multi-platform basis is paramount. Although participants used one or more security measure on their devices, such as Anti-Virus software and passwords, they fall foul in using it safely. This is apparent as the majority of them failed to utilize a strong password, employed password reuse and canceled or postponed a security related update.

Encouragingly, the results of this survey demonstrated that some of the reasons behind participants varying behavior risk levels are related to variations in age, gender, IT background, IT service usage and personality traits. It was found that IT professionals, although did not practice good behavior as expected, were in lower risk than non-IT professionals. Even in those practices in which they shared the same risk level, such as clicking on links/attachments within an email from unknown sources, non-IT professionals were in higher risk.

Whereas for age variations, it was found that the older the user the lower the risk. This is in line with the risk taking behavior of younger users as 38% of cybercrime victims were users in the age group 18-30 (Statista.com 2013). However, this does not imply that the older the user the more security minded he is, but could be due to reasons such as using the Internet less.

Regardless of the findings that males use pirate software more frequently than females, it was found that males are practicing better security, thus in lower risk, than females for most of the assessed security behaviors. Further to that, females practiced password hygiene *lower* than males, do *not always* disable their wireless technologies when not using them, connected and engaged more in public WiFi networks and social networks, and showed more tendency to click on attachments and links in emails without checking regardless of the sender, to name a few of their risk taking behaviors. This may explain why they are more prone to phishing than males as found by (Sheng et. al 2010).

Due to their high online engagement , thus the higher the chances they may face security risks, one might expect that higher online engagement may result in higher risk but when their security behaviors were assessed no particular pattern was found. As a matter of fact, those with medium service usage maybe in higher risk than others especially that they practice most of password hygiene behaviors less, more inclined to open documents even if warned not to, click attachments within emails without checking, not to lock their workstations when away from desk or use a

password for their home computers and less frequently back up their files and scan USB sticks before using them. This suggests that the higher the level of service usage/online activity does not necessarily imply better security behavior.

Further to that, survey findings suggest that personality traits play a role in effecting the risk level of users. This said, it was found that those of the same personality trait do not practice security behaviors in the same way. As a matter of fact, the BFI score of each personality trait played a significant role in participants' risk taking security behavior. As the higher the BFI score of personality traits of Openness, conscientiousness, extraversion and agreeableness the more responsible they are, this was reflected positively on their security behaviors. Therefore, the lower the BFI score the higher the risk across most of the assessed behaviors. However, a converse relation was found in the case of neuroticism personality trait. It is worth noting, though, that differences in Extraversion BFI score was correlated with only one of the assessed behaviors. Thus, this maybe an opportunity to further explore this fact by conducting similar studies targeting users of this trait. Among all personality traits, those who were high in conscientiousness were found to be practicing security better than others, thus in lower risk. This suggest that the competence, order, dutifulness and self-discipline attributes of conscientiousness personality were mirrored in most of their security behaviors.

Moreover, the survey findings suggest that there are several areas where users need to be educated and their behavior continuously monitored and directed. As it is challenging to predict how users behave, especially when security in practice is different from security in abstract, it is critical to understand how users communicate with systems. This survey highlighted some factors that could be used to predict user's risk level. Hence, to get security right and to encourage good security behavior, systems should adapt to users instead of vice versa.

As it was found that user's may easily become victims of such attacks not only because of their insecure behavior but because technology is failing them (Ibrahim et al. 2010). Decisions such as using pirated software or opening attachments in emails should be monitored in near real time and alerting the user in an individualized and persuasive manner. Further to that, the consequences of such actions should be explained to him prior attempting to do such action and educated on how to do it right. Hence, arguably, instead of telling users what not to do, they should be taught how to safely do what they want. Additionally, these findings suggest that users are willing and looking forward to added and convenient security that copes with their needs and notifies them in real time and up-to-date information on how to behave securely in a user-dependent way that is mostly understood by them. Increased targeted security awareness and communication through understanding risk will arguably improve the security behavior and lead to reduced security risks.

4.7 Conclusion

The study has sought to further investigate the relationship between user's behavior (or specifically behavioral intent) and various user-centric factors. A more complete set of analyses across a wider set of behaviors and factors has provided a more appreciable understanding of what significant relationships exist. The results of this investigation has shown that the studied factors do play an important role in shaping user's behavior and risk level. Conscientiousness, agreeableness and openness personality traits all play a role across two-thirds of all behaviors. The study has also reaffirmed that age, IT proficiency and service usage also have an impact on behavior. By capitalizing upon this, end-users could be provided with more effective awareness based upon the risks they present to systems. Thus, by the development of solutions that adapt to these differences, whether in assessing risk or in communicating it to users, this may enhance the way in which users behave and transform them into security minded users.

Chapter 5 : Establishing a User-centric Risk Assessment and Response Model

5.1 Introduction

Having identified that a number of factors influencing user's risk-taking behavior, the aim of this research is to develop a novel approach that takes into account these factors when assessing security risks for users and communicating them in a timely and individualized fashion. Aside from the traditional "one-size-fits-all" solutions, the approach introduces a new platform independent model – User Centric Risk Assessment and Response (UCRAR). This proposed model is anticipated to provide a comprehensive framework for individually assessing and communicating risks especially with the continuously evolving threat landscape. As such, user's behaviors are continuously monitored and risks are assessed on both system and user level taking into account the influence of a number of factors on user's risk taking behavior. Then, an individualized risk profile is created and risks are communicated accordingly in a timely manner. Further to that, it acts as an individualized security awareness/education tool that will give the user the ability to better understand risk and make a security informed decision.

This chapter will discuss the system requirements in the following section followed by a detailed description of the UCRAR model in section 3. A demonstration of operational flow in the proposed framework and how processes interact with each other in section 4 precedes the conclusion in section 5.

5.2 System Requirements

The proposed model seeks to help users in assessing their behaviors, improving their security knowledge/behavior and giving them the ability to make an informed decision. In order for such system to be applicable, a number of requirements need to be identified.

Among the aforementioned findings of the previous chapters was that users, access a wide range of services from a number of different devices and platforms, thus, increasing the users' security risk level. Additionally, it was explained how user-centric factors were related to changing/influencing this risk level, the burden to be aware of such risks and how to protect form them. Therefore, the necessity for a user-centric risk assessment and communication approach that adapts to user-centric factors and can be used across services and technologies becomes more apparent.

Given the fact that users have usability issues related to security software that may result in them dumping it or at least, due to misuse, degrading its performance, the model needs to be flexible, user-friendly, usable, adapts to the user and speaks his language.

As the use of vulnerable software is considered a threat to the user, the system itself in terms of installed software should be assessed. Examples of such vulnerable software are a vulnerable Operating System and an out-of-date application. Not limited to application vulnerability, but the fact that malicious/pirate software originating from suspicious sources could be a possible threat. Consequently, the source from which the software originated should be considered. Further to that, connecting to the Internet could be of risk to the user especially with the increasing number of Internet users and how users are spending more time doing online activities. Thus, a vulnerable router could also be considered as a threat to the user. As such, risks should be assessed on the system level.

As user-centric factors were found to significantly relate to user's risk taking behavior, they should be considered when assessing risk. Hence, risks are not only assessed on the system level but also on the user's level. However, to keep the system up-to-date over time, a community based approach of risk data is required.

With this continuously evolving threat landscape where almost two million threats introduced on a daily basis (Symantec 2018), the fact that users only try to protect themselves from risks apparent to them and that they are, arguably, unwilling to constantly learn about information security comes the need for an individualized security risk assessment/awareness approach. Not limited to that, but user's behaviors need to be continuously monitored and timely assessed. Prior literature largely focuses on one-size-fits-all solutions and, arguably, this does not provide the granularity required for the individual users. Therefore, the proposed model needs to go beyond the traditional solution to adapt to user's needs and constantly monitor and assess his behaviors against good or expected behavior to generate an individualized risk profile. Then, these risks are communicated in an individualized persuasive manner and targeted security education/training is provided accordingly.

Nevertheless, this continuous monitoring of user's behaviors does have some ethical implication. From an ethical perspective, it is important not to violate any privacy rights of the user. An important aspect is that users need to trust the system and that this continuous monitoring is motivational and not invasive. Hence, if this continuous monitoring is done without user's consent, it will be considered a breach of privacy. Therefore, users need to be aware that this continuous monitoring is done for their own protection and will not violate their privacy. However, this practice is subject to regulations of current standards and laws. The General Data Protection Regulation (GDPR), which was enforced in May 2018, has 99 articles that are concerned with working practices in the way that personal data is used, handled and shared (General Data Protection Regulation 2019). In compliance with GDPR, user's consent to the use of their data is obtained when installed the application. This is done by having the user accept an agreement terms in an understandable, jargon-free and accessible way. In this agreement, it is clarified to the user that data is not shared with any other application. Additionally, the continuous monitoring of

user's behavior and any collected data will not be used for purposes other than those intended for risk assessment.

To this end, the proposed model is based on two components, risk assessment and risk communication. For the former component to operate, it requires access to a number of databases/repositories. Particularly, a database/repository of good/expected behavior, community-based risk data and a vulnerability database that are created and managed by third parties such as an ISP, Network operators, the Government or big companies such as Google and Microsoft. Although the implementation of such databases is outside the scope of this research, their functionality will be explained in the following section. Additionally, a personality and a learning style test tool is needed to determine the user-centric factors of personality trait and learning style. For the latter component, an Internet-based body of knowledge is needed as a source for required security awareness/education materials. However, to avoid overwhelming the user with redundant risk-related messages, those that are issued by this system or other applications are recorded so that a similar message will not be issued twice, i.e. from UCRAR and from other installed applications.

5.3 The UCRAR Framework

In the literature, many risk assessment methodologies were found as discussed in Chapter 2. However, they tend to assess risks either on the software/application level, based on assets and applicable threats, or permissions that are requested by each application prior to installing it, as in mobile devices for instance. Opposed to other risk assessment methodologies that utilize experts opinions, methods such as those proposed by (Ledermuller and Clarke 2011) and (Theoharidou et al. 2012) employ user input resulting in a personalized risk assessment. However, this user involvement could be considered as a burden on the user, especially if the number of installed software/applications is numerous, that may result in him dumping/rejecting the risk assessment

software/application. Moreover, the quality of the risk assessment maybe affected by the varying input details reflecting different users' characteristics, namely, their IT expertise and skills.

Many types of data are stored on users' devices such as photos, contacts, documents and messages that are accessed by different applications. However, the unauthorized modification or disclosure of this data may result in a number of undesirable consequences on the CIA and privacy of such data. As each application has different impacts on data, which implies that the risk level is changing within the application. Actually, different processes within an application have different impacts, thus, generating different risk levels for the same application. As a result, no single risk level could be assigned to an application. Not limited to that, but the way in which the user uses these processes may escalate or de-escalate these risk levels. For example, in the HSBC mobile application, user's behaviors where there is no sharing of user's data as in reading products, services and offers has no impact on data. Thus, from an application based behavioral perspective, risk is kept to a minimum. However, this risk level could escalate when combined with other non-app related behaviors such as connecting to a public Wi-Fi network or using a non-updated version of the application. Another example is the process of adding a photo in the Facebook application. On the one hand, adding a photo of The London Eye, for example, has a *low* risk level whether the user's account is public or private. Whereas adding the same photo with location data may have an impact on user's privacy, thus, escalating the risk level to *medium* in a private account and possibly to *high* in a public account. On the other hand, for the same process of adding a photo but of the user's child, for example, in a private account has a *medium* risk level that escalates to *high* when the account is public. These examples serve to demonstrate that the risk level of user's behaviors within an application process could change when combined with other behaviors within the same application. Thus, arguably, assessing the risk level based on user's behavior may result in a more realistic and accurate assessment. To the best of the researcher's knowledge, assessing and

calculating risk for each user behavior of each process within an application and combining it with other behaviors simultaneously, and using user-centric factors such as demographics, online activity, personality traits and IT expertise as additional risk factors to create a user-centric risk score/level has not been investigated yet. Moreover, combining this user-centric risk assessment with system-level risk assessment to create an individualized risk profile is a novel approach to information security risk assessment.

Consequently, the proposed methodology for assessing security risks will be based upon continuously assessing and calculating risk on both system and user level and an individualized risk profile will be created accordingly. Additionally, risk information from a third party that is based on a large population, i.e. community-based, is used in the risk assessment. Therefore, the novelty of this proposed model, UCRAR, depends upon three significant aspects: monitoring and assessing user's behaviors, monitoring and assessing the system from which the user is working and individually/persuasively communicating risks. Hence, UCRAR is composed of two main components as in Figure 5.1. Namely, the Risk Assessment component and the Risk Communication component.

In the first component, user's behaviors are monitored, security risks are assessed and an individualized risk profile is created accordingly. Whereas the second component is mainly concerned with receiving the individualized risk profile, analyzing it and communicating the risk in an individualized manner. As part of the novelty of this proposed framework, user-centric factors are utilized, among other factors, in both components.

Actually, in the Risk Assessment component, the assessment is not limited to assessing risks on system level such as installed software/apps, but user's behaviors will be continuously monitored and assessed against good or "expected" behavior. Consequently, user-centric factors are used to generate a risk profile that changes and is individualized to users. Further to that, risk information

from a third party that is based on a large population, i.e. community-based, is used in the risk assessment. As a result, the aggregated final risk score/level is a quantitative value between 0-low risk and 10-high risk and passed as part of the individualized risk profile to the second component of UCRAR. From this point, the terms software and application will be used interchangeably to refer to any piece of software installed on user's device.

In the Risk Communication component, the risk profile is analyzed. Based upon that analysis, it decides on the most suitable individualized, persuasive form of communicating this risk to the user and how to enhance his security knowledge. Additionally, topics in which the user needs further education will be internally identified and, as a result, individualized security training and awareness that adapt to user-centric factors will be provided in the user's preferred learning style such as an educational security game for teen agers.

To this end, UCRAR will continuously monitor, assess, communicate and educate users of security risks that relate to them in an individualized persuasive audio/visual manner to convince the user to change his behavior, be "security-minded" and give him the ability to make an informed decision. To accomplish this, the following processes are established:

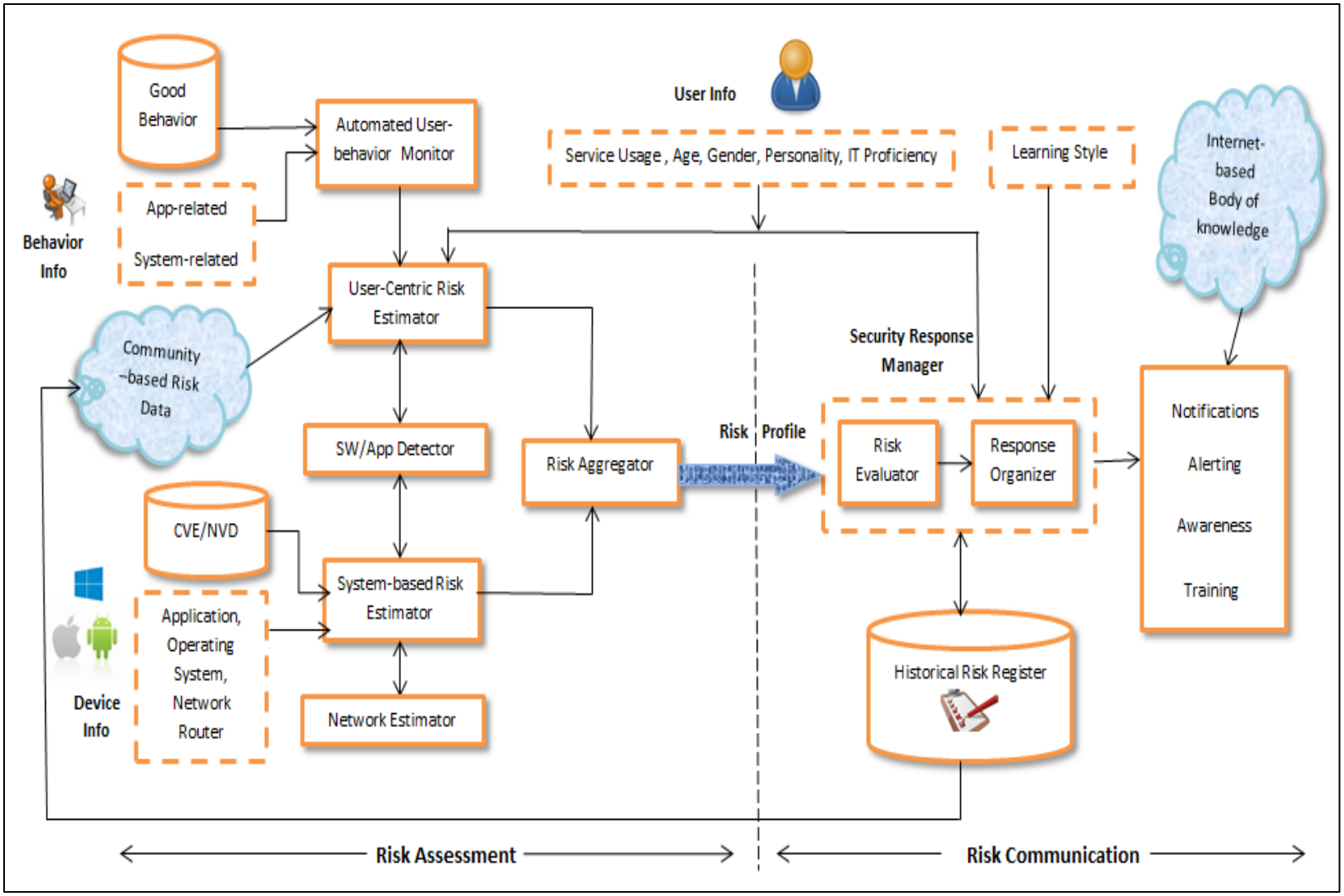

Figure 5.1: The User-centric Risk Assessment and Response, UCRAR, Framework

5.3.1 Risk Assessment Component

For this component to carry out its functionality, the following processes are established:

5.3.1.1 Software Detector

The risks of a vulnerable/out-of-date application and those originating from an illegitimate source have been previously explained in this research. However, there are millions of software products in the world. For example, the number of applications in Google Play store increased from 400.000 in 2011 to 3.5 million in 2017 with an average of almost 6000 applications released on a daily basis (Statista.com 2017). However this fails to consider the existence of organizational application. Many applications could be installed on the user's device with varying consequences on the CIA and privacy of user's data.

To individually risk assess each installed application would be a time consuming task. Thus, the aim of this process is to detect all installed software on user's device and assign a quantitative score/weight to each detected software. This score could be determined in many ways such as level of application/service usage or type of application/service such as banking, messaging or social networking. Additionally, it could be determined in terms of its CIA impact. To reduce the burden on the user in individually scoring each installed application, the categorization approach proposed by (Ledermuller and Clarke 2011) is adopted. In this categorization approach, applications are classified into groups according to their type/usage and each group is assigned a certain weight. This weight assignment will be part of system startup/configuration where each group will be assigned a quantitative value by asking the user explicit questions of how important this group to him.

To avoid user's confusion when using a large scale, a scale of 0-**very low** to 4-**very high** will be used. Then, each detected application will be mapped into its corresponding group and assigned a score accordingly resulting in an *app-score*. For example, applications are classified but not

limited to as in Table 5.1. Further to that, application version, *app-ver*, and the name of the source/market from which the application was installed from, *install-name,* are detected (if any).

Social networking	e-banking	e-mail
Messaging	Maps and navigation	Entertainment (games, music …etc)
News	Shopping	Office applications (Ms Word, Ms Excel …etc)
Photography	Security	Operating system
Web access		

Table 5.1: An Example of Software/Applications Groups

Thus, the output of this process is the following tuple

Sw-info = (*sw-id*, *app-score*, *install-name*)

where: *sw-id* is the software/app ID in Common Product Enumeration CPE

5.3.1.2 Good (Expected) Behavior

To individually assess each behavior, a clear description of a good user behavior to compare it against the current user behavior has to be determined. Since it is difficult to include all expected/good behaviors, this knowledge base will include a set of descriptors that suggest what good behavior should be in a certain aspect and used as a reference for user security compliance. In password hygiene, for instance, a list of good behaviors related to passwords will be provided such as :

- Use of a strong password, i.e. at least 8 characters long with a combination of capital and small letters, numbers and special characters.
- Password is not recycled in which the same password is used for multiple accounts
- Frequency of changing passwords, every three months for example
- Not allowing web browsers/software/apps to store passwords

5.3.1.3 User Behavior Monitor

With this continuously evolving threat landscape and the wide range of computing platforms and services accessed, the need to continuously monitor and assess user's behaviors in a timely manner becomes more apparent. Certain users' characteristics were related to changing/influencing

his risk level, as discussed in Chapter 4, suggesting that user's characteristics need to be gathered. Hence, the functionality of this monitor is a two-fold:

I. To continuously monitor user's behavior independently of the used software/app and compare it against good/expected behavior. This is timely done and is event triggered. For example, if a user is to close a browser/app, he will be reminded to sign off from online service before closing. These monitored behaviors may include, but not limited to:

- ✓ Information posted on social networks
- ✓ Opening attachments/links in emails without checking them
- ✓ Connecting to public access WiFi networks
- ✓ Backing up data
- ✓ Using a USB drive without scanning it
- ✓ Opening a document/link despite security warnings
- ✓ Downloading files from suspicious websites
- ✓ Locking workstation when away from desk
- ✓ Disabling wireless technologies when not used
- ✓ Logging off from online systems before closing the browser
- ✓ Disabling AV/firewall
- ✓ Cancelling or postponing a security related update
- ✓ Installing pirate software

II. To collect user information in terms of the specified user-centric factors. This data collection is done in three ways, namely, explicitly, implicitly and by taking a specialized test as in Table 5.2. The categories of the user-centric factors of age and gender are determined by asking the user explicit questions. Based on the results of a personality and learning styles tests such as the Big Five and the VARK learning style test, the user-centric factors of personality and learning style are determined and the user is assigned a factor category accordingly. This user-info data collection

is considered as part of system setup/configuration. The User Behavior Monitor will automatically and transparently detect and measure the following user-centric factors :

- ***IT proficiency level***: A number of metrics will be used to determine user's IT proficiency level such as settings and modification of web browser configurations, frequent use of shortcut keys and the use of advanced features in software/apps such as section breaks and cross sections in MS Word and macros in MS Excel. Accordingly, the user will be assigned an IT proficiency level of either professional or not.
- ***Service usage***: A number of metrics will be used to determine user's level of online activity and service usage such as number of services utilized and number of times these services are accessed on a predefined basis. Accordingly, the user will be assigned a service usage level of high usage, medium usage or low usage.

However, for IT proficiency and service usage level user-centric factors the worst-case scenario is adopted. The categories whom found to be in highest risk, as in findings of Chapter 4, are assumed as default values, i.e. non-IT professional and high service usage. As the user is using the system, his behavior is monitored and these categories will be adjusted according to a predefined set of metrics.

User-centric factor	Description	Determined
Age	Users will be classified into three age groups: 18-30 years, 31-50 years and 51+ years	Offline. By explicitly answering a direct question, as part of system setup/configurations
Gender	Users will be classified as either male or female	
Personality	According to their BFI score users will be classified as either high or low in one of the personality traits of Openness, Conscientiousness, Extraversion, Agreeableness and Neuroticism.	Offline. By using a BFI tool, as part of system setup/configurations
Learning style	According to their preferred learning style, users will be classified according to their VARK learning style	Offline. By using a LS tool, as part of system setup/configurations
IT level	According to predefined metrics to measure their IT expertise, users will be classified as either novice, intermediate or advanced	Online. Determined internally by the User Behavior Monitor as described in section 5.3.1.3
Service usage	According to a predefined metrics to measure their service usage and online activity, users will be classified as either high usage, medium usage or low usage	

Table 5.2: Settings of User's-centric Factors

Thus, the output of this process is the following tuple

B-info = (*B-expected*, *B-actual*, *U-info*)

Where*:* *B-expected* is the expected good behavior derived from the Good Behavior knowledge base

B-actual is user's current behavior

U-info is user-centric factors expressed as the tuple = (IT-level, Use-level, Age, Gender, Personality, Learning-style)

Where*: IT-level* Є {IT-pro, non-IT}, where IT-pro= IT professional, non-IT = Non-IT professional

Use-level Є { $High_{use}$, $Medium_{use}$, Low_{use}}, where $High_{use}$= high usage, $Medium_{use}$= medium usage, Low_{use}=low usage

Age Є {Low_{age}, $Medium_{age}$, $High_{age}$}, where Low_{age}= 18-30 years old, $Medium_{age}$= 31-50 years old, $High_{age}$= 51+ years old

Personality Є {HO, LO, HC, LC, HE, LE, HA, LA, HN, LN}, where HO, for example,= High BFI in Openness personality and LE = Low BFI in Extraversion

Gender Є {female, male}

Learning-style Є {V, A, R, K} where V = visual, A = auditory, R = read/write, K = kinesthetic

5.3.1.4 User-Centric Risk Estimator

This process performs a mapping of user behavior to software/apps. Hence, what is the user doing against what software given that a threat against a software maybe increased by user's *insecure* behavior. For example, if a user was logged into an online service and attempts to close the browser, the User-Centric Risk Estimator will map it to the current used application which is an online banking application that was detected by the software detector. Consequently, a quantitative risk score between 0-low risk and 10- high risk will be determined after assessing user behavior

given the previously mentioned data. This risk score is calculated according to a proposed model as will be explained in the next Chapter. As a result of this mapping/calculation, a behavioral risk score, *behavior-risk*, will be calculated and passed to the Risk Aggregator. Thus, the output of this process is:

behavior-risk, the quantitative behavioral risk score, $0 \leq behavior\text{-}risk \leq 10$.

5.3.1.5 Community-Based Risk Data

The proposed UCRAR is based upon user's behaviors from the user survey of Chapter 4 in a certain point of time. Once the proposed system is running with many people using it, there is the chance to look at their user-centric factors, behaviors and responses in real time on a continuous basis. Information about users, behaviors and responses are fed into this Community-Based Risk Data in an anonymized form on a continuous basis. Hence, those found statistically significant correlations could be re-evaluated and the user-centric risk estimation will be modified accordingly. For example, if the user-centric factor of age no longer has a statistically significant correlation with a certain behavior or a new user-centric factor becomes significant for a behavior the system will adapt accordingly. The system has all required information to do this so called re-evaluation by mapping user's actual responses to a more meaningful risky/non-risky decision. Hence, replacing the survey data with measured data from users. This will allow the system to move beyond the static point in time to a continuous understanding of these factors and correlations. Therefore, by knowing the actual behavior and response, those found significant correlations will be truly significant.

With the continuously evolving threat landscape, new threats might be introduced and impact a behavior quite differently depending on user-centric factors. As such, those relations are periodically revised such as every six months. Not limited to that, user's responses will be periodically used to intelligently re-measure user-centric factors. For example, user's age is

recalculated to ensure he belongs to the assigned age category or reassign him accordingly. Or a user's IT-level could be changed from a non-IT professional to an IT-professional based on his behavior and so on. These examples serve to demonstrate that UCRAR can dynamically adapt to changes in user-centric factors.

Hopefully, this process will be used as feedback mechanism to keep the system up-to-date without having to re-run the survey and gradually move away from behavioral intent to actual behavior. Further to that, by measuring these responses, this process will have a smoothing effect on generated risk score/level by moving away from grouping of user's (based on survey results) to a more personalized risk model. Similar to the knowledge base of good/expected behavior, this community-based risk data is a centralized web service managed by a third party such as ISP, network operator …etc.

5.3.1.6 Network Estimator

Given that a vulnerable router is more likely to be exposed and used as a threat source, this process monitors the status of the network in which the user is connected to and is kept to a minimum level. Information about the used network devices, i.e. routers, are collected and passed to the System-Based Risk Estimator. Router information will be expressed in terms of router's software name and version and passed to System-Based Risk Estimator to check it for vulnerabilities. Thus, the output of this process is the parameter *r-id* which is the ID of the software executed on the router in CPE

5.3.1.7 System-Based Risk Estimator

A vulnerable software could be exploited by attackers compromising the system where this software is running such that the more vulnerabilities in a software/app the less secure it is and, eventually, the lower its trustworthiness level. Hence, a vulnerability-oriented approach (NIST 2012) where the method starts with the identification of a set of vulnerabilities is used. This process analyses and calculates security risks on system level. As perfect security is considered to be

unachievable for information systems, then the goal is to achieve a security level that is deemed appropriate to user's needs and requirements. This is accomplished by checking all installed software, router software and also platform information in terms of the used Operating System for vulnerabilities. For each of the previously mentioned, the System-Based Risk Estimator will check vulnerabilities knowledge bases such as NVD and CVE for known vulnerabilities and calculate a software risk score accordingly. The final system risk score, *system-risk*, will be calculated based upon a proposed model as explained in the next Chapter. Thus, the output of this process is:

system-risk which is the quantitative system risk score, $0 \leq$ *system-risk* ≤ 10.

5.3.1.8 Risk Aggregator

The purpose of this process is to evaluate/assess security risks based on information obtained from User-Centric Risk Estimator and System-Based Risk Estimator and generate a risk profile that adapts to users accordingly. Hence, this risk profile is composed of a set of parameters that are required by the Security Response Manager to do its job. This aggregator will assess and analyze the security risk and determine the final risk score according to a proposed model as will be explained in the next Chapter. However, the quality of the risk assessment depends on the accuracy and granularity of data provided by the previously mentioned processes. Thus, a risk profile will be generated as follows:

Risk-Profile=(*B-actual*, *U-info* ,*overall-risk* ,*risk-level, date*)

Where:

Overall-risk quantitatively expressed and calculated overall risk score, $0 \leq$ risk-score ≤ 10

risk-level is the level of final risk score expressed qualitatively $\in$ {h, m, l}

date is the date and time stamp this behavior was performed.

5.3.2 Risk Communication Component

The second component of the framework, Risk Communication, starts by receiving the risk profile from the Risk Aggregator, analyzing it and deciding on the best targeted form of communicating the risk to the user. The importance of communicating risks in a persuasive and individualized fashion has been previously discussed in Section 3.7. To this end, the aim of this framework is to convert the user from arguably being ill-informed into a security minded user who is able to make an informed decision. The proposed way to accomplish this is, as previously discussed, by continuously monitoring, assessing user's behaviors and to use persuasive risk communication in the form of individualized messages to give the user an opportunity to make a security informed decision. In addition, subjecting the user to targeted security awareness/education to influence his behavior to be more secure.

Unlike employees of an organization, users have no security policy to comply to nor an enforcement of security education. This lack of education enforcement may be one of the reasons behind this insecure behavior. In addition, there is the challenge of convincing the user of his responsibility to protect himself (Kritzinger, Von solms 2010). Based on user's risk score/level, two broadly potential behaviors are recognized. Namely, secure and insecure behaviors as follows:

- ✓ **Secure behavior**: The user is behaving in a good/safe manner, thus his risk level is low.
- ✓ **Insecure behavior**: The user is at risk whether this behavior is done intentionally or unintentionally. The risk level of this behavior is either medium or high.

The reasons behind these behaviors were established especially the fact that user's behavior is hard to predict and there is the case of an aware user that simply chooses to behave insecurely. In addition, different types of user's classifications were previously discussed in Section 3.5. As such, two broad user's categories could be identified according to their insecure behavior as aware and unaware. However, many user's categories could be identified in between. The timing of the

behavior, for example, could be used as an indicating factor when categorizing users. For example, a user that was alerted for an insecure behavior, then, after a long period of time he performed the same behavior. This could be as a result of him forgetting about the insecurity/consequences of this behavior. Thus, the time period between these behaviors could be used as one of the reasons behind this insecure behavior. Consequently, a third category of users, the forgetful, could be identified. The user-centric factor of service usage could be used when determining this time factor. Given a certain window of time, the rate of using the Internet varies from high as in high usage users to low as in low usage users. Three time periods are suggested as short, medium and long. However, the duration of each of these periods is different according to the user's service usage level. A suggested categorization of such periods is as in Table 5.3. However, according to data provided by the User Behavior Monitor on the user's service usage level, this will be adjusted accordingly. Hence, the following user's categorization will be used when assessing their insecure behaviors:

I. **Unaware user:** A user who has done this behavior for the first time and the risk of it may be unknown to him.

II. **Aware user:** A user who has repeated the same behavior within a short time period. Thus, the user maybe aware of this insecure behavior and its consequences but simply does it again. This may be interpreted as intentional insecure behavior.

III. **Forgetful user:** A user who has previously done this behavior but within a medium or long time period. Hence, the user maybe aware of this insecure behavior and its consequences but forgot about it due to time duration. This may be interpreted as unintentional insecure behavior.

However, whenever a behavior is performed more than once, the difference between behavior's risk scores could be used to further explain user's insecure behavior.

Service usage level	Time period			Time span
	Short	Medium	Long	
Low	0 days..30 days	31 days ..60 days	61 days ..90 days	Three months
Medium	0 days ..20 days	21 days .. 40 days	41 days .. 60 days	Two months
High	0 days .. 10 days	11 days .. 20 days	21 days .. 30 days	One month

Table 5.3: Suggested Categorization of Time Period

Evidence suggests that static risk communication may result in users becoming inattentive to messages delivered (Wash 2010; ; Blythe et al. 2011; Wash and Rader 2011; Blythe and Camp 2012; Wahelberg et al. 2013). Thus, the robustness of risk communication should be suited to the encountered risk by providing timely information to the user about their risk taking behavior. To overcome the challenge of convincing users to avoid risks, changing their behavior to promote good practice and to improve the effectiveness of persuasive technology, three response approaches will be used. It is anticipated that the utilization of such approaches will facilitate targeted risk communication, prevent habituation and change risk perception of users. These approaches utilize a blocking and a non-blocking mechanism. In a blocking approach, an explicit decision is required from the user where he is banned from doing any further activity until this blocking dialog is confirmed. Whereas in a non-blocking approach, an alert is shown for a certain period of time then disappears without preventing the user from doing his current activity nor his need to confirm it. The advantages and disadvantages of using each of these approaches are appointed in the security literature. For instance, the former could be dismissed without the user noticing the contents and the latter may simply be overlooked (Maurer et al. 2011). One way to overcome these disadvantages is not to rely on a single mechanism but on a combination of them that differs according to response severity. Additionally, between these two extremes, a proposed semi-blocking approach could be used. In this approach, explicit attention is required from the user as an alert is shown to him but does not stop him from performing his current activity. To attract user's attention, sound will be used in a discontinuous manner. To dismiss it, it needs to be confirmed. This will make the user continue with his current activity before dealing with the alert. All of the

previously discussed factors will be considered when communicating risk to the user. To accomplish this proposed risk communication, the following processes are established:

5.3.2.1 The Security Response Manager

Based on the user's behavior risk level, the Security Response Manager will make a decision on what the next step is. However, when communicating risk to the user, The Security Response Manager will decide upon the best way to do that. The best form of persuasive technology that best suits the user will be decided upon and used based on U-info that is part of the risk profile. Security is "rarely the user's primary goal" and users only try to protect themselves from risks salient to them (Blythe and Camp 2012). Thus, to educate user's about security risks and promote good behavior, user-tailored messages that take into account the individual user-centric factors are used. Two sub-processes carry on the functionality of The Security Response Manager as follows:

* **Risk Evaluator**: Once the risk profile is received, the behavior's risk level is checked first. If the behavior is secure, i.e. low risk, then behavior-response-information is sent immediately to the Historical Risk Register. If the behavior is insecure, i.e. risk level is medium or high, then the risk profile is forwarded to The Response Organizer.

* **Response Organizer**: Prior to issuing a message, it will check the Historical Risk Register of previous incidents of the same behavior and the issued security messages related to it. Hence, the response mechanism of this process depends on two concepts, namely, informing the user of his behavior's risk score/ level and deciding on the best way to communicate/educate the user about his risk-taking behavior. Hence, based upon the information received in the risk profile and historical data about the same behavior (if any) from the Historical Risk Register process, a gradual, individualized and persuasive response mechanism is proposed as in Figure 5.2 .

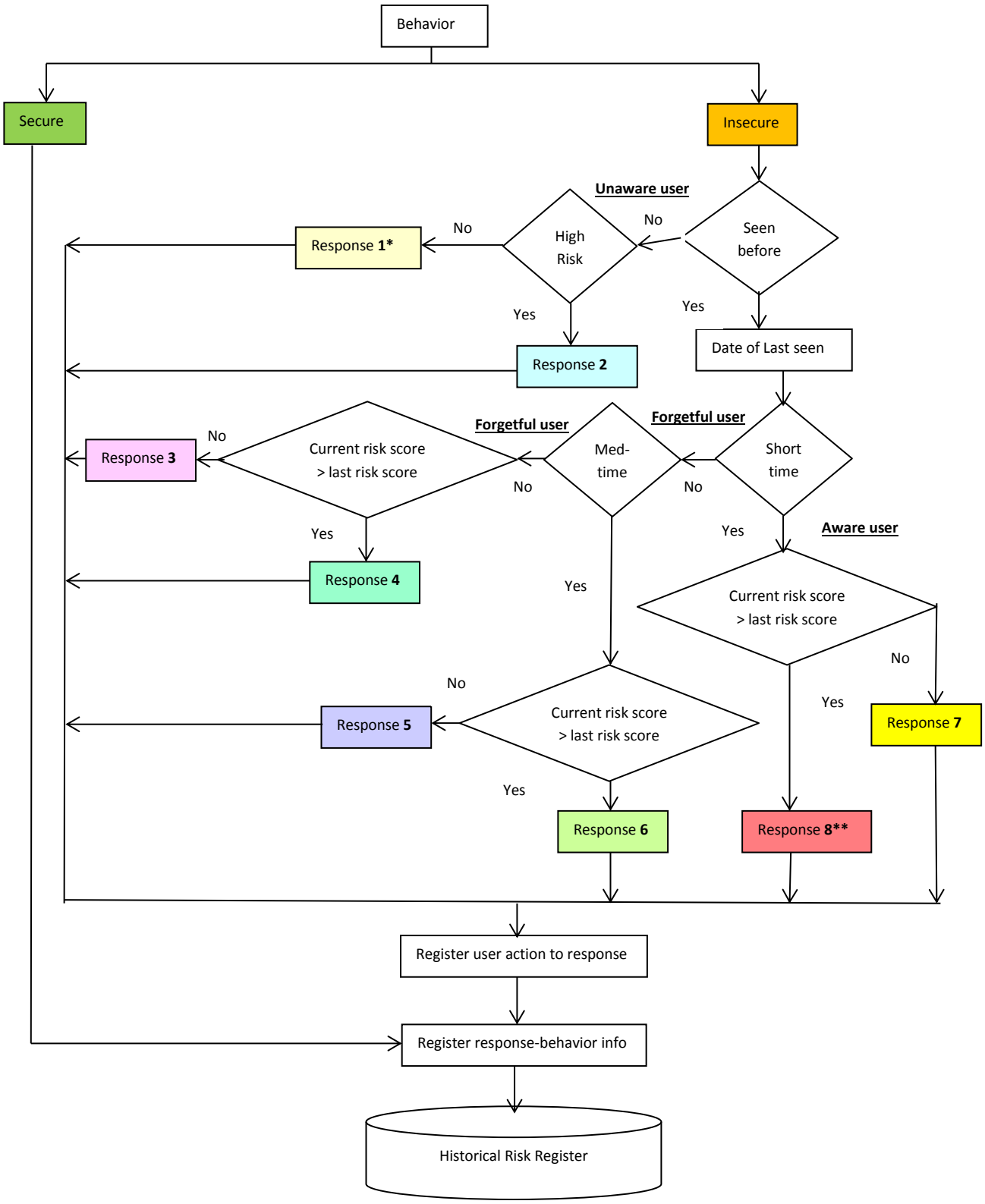

Figure 5.2: The Response Mechanism

*Lowest response level, ** Highest response level

Educating users about information security is a challenging but a must to fight against this continuously evolving threat landscape. As discussed previously in this research, although a number of traditional techniques are used to educate users, but unfortunately failing as users tend to ignore threat warnings. Furthermore, the traditional one-message/one-size-fits-all approaches to risk communication, for example, should be replaced by a targeted approach that goes beyond just informing the user. This targeted approach should focus on the user, stress on his responsibility to protect himself, provide him with information on what to do and provide some level of security education in an individualized persuasive and timely manner. However, this combination should be used cautiously to avoid overwhelming the user with information and help in motivating continuous secure behavior. Therefore, a response mechanism is proposed that is intended to create an information security literacy by creating a baseline of information security culture. Hence, instead of just warning the user once of his insecure behavior, six response levels are proposed and to be used in a gradual manner. The risk score, number of times a behavior was performed and time period are all factors used to leverage the response level as shown in Table 5.4. These response levels are:

1) **Level 1 (Response 1):** This is the lowest response level. In this level, a basic awareness message tailored to user's personality trait is given in a blocking approach.
2) **Level 2 (Responses 2 and 3) :** A basic awareness message tailored to user's personality trait is given in addition to information about what others are doing in the same situation/ a statistics about the consequence(s) of this behavior. A blocking approach is used.
3) **Level 3 (Responses 4 and 5) :** Similar to Level 2. Additionally, to continuously raise user's awareness, a further reminder of these consequences and what to do are given in a non-blocking approach.

4) **Level 4 (Response 6) :** A basic awareness message tailored to user's personality trait is given in addition to information about what others are doing in the same situation/ a statistics about the consequence(s) of this behavior. An *awareness* module related to his current behavior and in the user's preferred learning style such as watching a video, is recommended to the user in a blocking approach. To continuously raise user's awareness, a further reminder of these consequences and what to do in a non-blocking approach is used. If the user cancelled or postponed the recommended module, he will be reminded of it using a semi-blocking approach.
5) **Level 5 (Response 7):** Similar to level 4, but instead of an awareness module, a *training* module related to his current behavior and in the user's preferred learning style such as playing a security game, is recommended to the user.
6) **Level 6 (Response 8):** This is the highest level of response. Similar to level 5 except that If the user cancelled or postponed the recommended module, he will be reminded of it using a blocking approach.

As no enforcement of security education could be made on the user, the reminder approach is used. Firstly, it is used as means for providing further education about user's behaviors. Secondly, when a user cancels or rejects a recommended security education module, the reminder approach is used as a "remind me later" option. Nevertheless, there is the case of him cancelling or postponing several recommended modules. In this case, they are arranged in a descending order according to how frequent these behaviors were committed in a time period. To avoid bombarding the user with reminders and alerts, it is suggested that the recommended security education module related to the most frequently done behavior supersedes the others. Further to communicating risks in a visual/audio manner, passive security messages that are integrated within software/app will be provided. Moreover, the user will be given the option to be notified by email/SMS sent to his cell phone such as reminding him to change his Library online account password or to logoff from the

Employment Service account. A summary of these response levels is as shown in Table 5.4 given that security education is always given in a blocking response approach.

	Security Education				Reminder's Response Approach		
Response Level	Basic awareness	Statistics/ consequences	Awareness module	Training module	Blocking	Non-blocking	Semi-blocking
Level 1	√	-	-	-	-	-	-
Level 2	√	√	-	-	-	-	-
Level 3	√	√	-	-	-	√	-
Level 4	√	√	√		-	√	√
Level 5	√	√	-	√	-	√	√
Level 6	√	√	-	√	√	-	√

Table 5.4: Response Levels

In these response levels, user-centric factors of personality traits, age, IT-proficiency and learning styles are considered when communicating risk to the user. Little evidence is found relating the effect of security messages of various behaviors to gender. The study by Sheng et al. (2010), for example, has shown that females have a stronger tendency to reply to phishing emails than males. This could be extended to include more security behaviors. However, no specific evidence was found that relates the service usage level to security messages nor to security education. The authors of (Kazjer et al. 2014) found that messages tailored to user's personality trait could increase its effectiveness and minimize a backfire response. The message themes and related personality traits are as shown in Table 5.5.

	Personality Traits				
Message Themes	Extraversion	Agreeableness	Conscientiousness	Openness	Neuroticism
Deterrence	-	√	-	-	√
Morality	-	√	-	-	-
Regret	-	√	-	×	-
Incentive	-	-	-	×	-
Feedback	√	√	√	×	√

Table 5.5: Personality Traits and Message Themes (Kazjer et. al 2014)

√ more receptive, × less receptive

Each personality trait is more receptive to one or more message except for the personality trait of Openness. Apposed to other personality traits, openness was not more receptive to any message theme. Actually, it was less receptive to regret, incentive and feedback messages. As such, these themes will not be used for a user with an openness personality trait to avoid a backfire response. Consequently, it is suggested to use deterrence and morality message themes when responding to an openness personality trait user. For the behavior of " Using pirate software", for example, the same security message could be written in five different ways through the manipulation of words as follows:

- **Deterrence**: Using illegitimate software can result in criminal prosecution and a fine of thousands of Pounds.
- **Morality**: Using legitimate software is the right thing to do and complies to secure/safe security behavior.
- **Regret**: Illegitimate software maybe malicious. Imagine how bad you feel if your computer gets a Virus and crashes.
- **Incentive**: When using legitimate software, Software companies will frequently give you technical support, gift cards and promotions.
- **Feedback:** Almost 70% of computer users do not use illegitimate software. You should join them to be security conscious.

In addition to the previously mentioned design factors, a number of design concepts are suggested when responding to the user about his insecure behavior. These are, but not limited to, as follows:

- ***Physical mental models***: Evidence suggests that mental models were found to be more accessible by the user (Blythe and Camp 2012; Camp 2006). Hence, an approach of

embedding graphics and visual indicators within security messages will be used. Particularly, the use of physical mental models to change users risk perception.

- ***Messages that speak the user's language:*** Given that users do not react to security messages in the same way, messages that speak the user's language will be used. Thus, persuasive messages that adapt to user's characteristics will be determined and delivered. For example, a message displayed to a novice user should be jargon free, in contrast to a message displayed to an IT expert user. Moreover, personality based risk communication strategies will be utilized in which messages will be tailored to user's personality trait as explained earlier.
- ***Colors and sounds***: Colors will be used to attract user's attention by using the traffic light terminology. Accordingly, risk level will be expressed in color (red for high risk, orange for medium risk and green for low risk), quantitatively (scale 0..10) and qualitatively (high, medium and low). A user who is overwhelmed with his work may not notice or ignore the security message, as a result, sounds will be used as a second form of attracting user's attention in the semi-blocking approach.
- ***Minimalist consistent design***: To avoid overwhelming and distracting the user, more details about the behavior and what to do are provided by clicking on a " More Info" button in the alert (Ibrahim et al. 2011). When clicked, the dialog box will expand to include more details. From a usability perspective, the placement of buttons in the alerts such as "OK" and "More Info", are consistent regardless of the response level.
- ***Animated avatar:*** The security status of both system and user behavior will be continuously monitored and visually expressed in the form of an animated avatar. This avatar will wave a flag, for example, that changes its color according to the current risk level. If the user wishes for further detail, a balloon that briefly describes the risk status will be displayed when this avatar is clicked.

- ***Behavior report***: Similar to the concept of an Ant-Virus software monthly report, a periodic report is issued to the user describing his behavior in that period. This will be in the form of a graph showing the number of times the user was in each risk level, number of issued alerts and the number of accepted/rejected alerts. Further details could be offered by clicking on a "More Info" button. As a form of motivating the user, an awareness meter is proposed. The mechanism of such meter is that if the user is not warned /obeyed immediately all displayed security messages in a short period of time, he will be awarded by sharing this success with his friends on Facebook, Twitter… etc. or with other users of this system, i.e. being in the community leader board.

As this proposed framework is multiplatform, Figures 5.3,5.4,5.5,5.6 and 5.7 are suggestive and not definitive designs of alerts generated by The Security Response Manager.

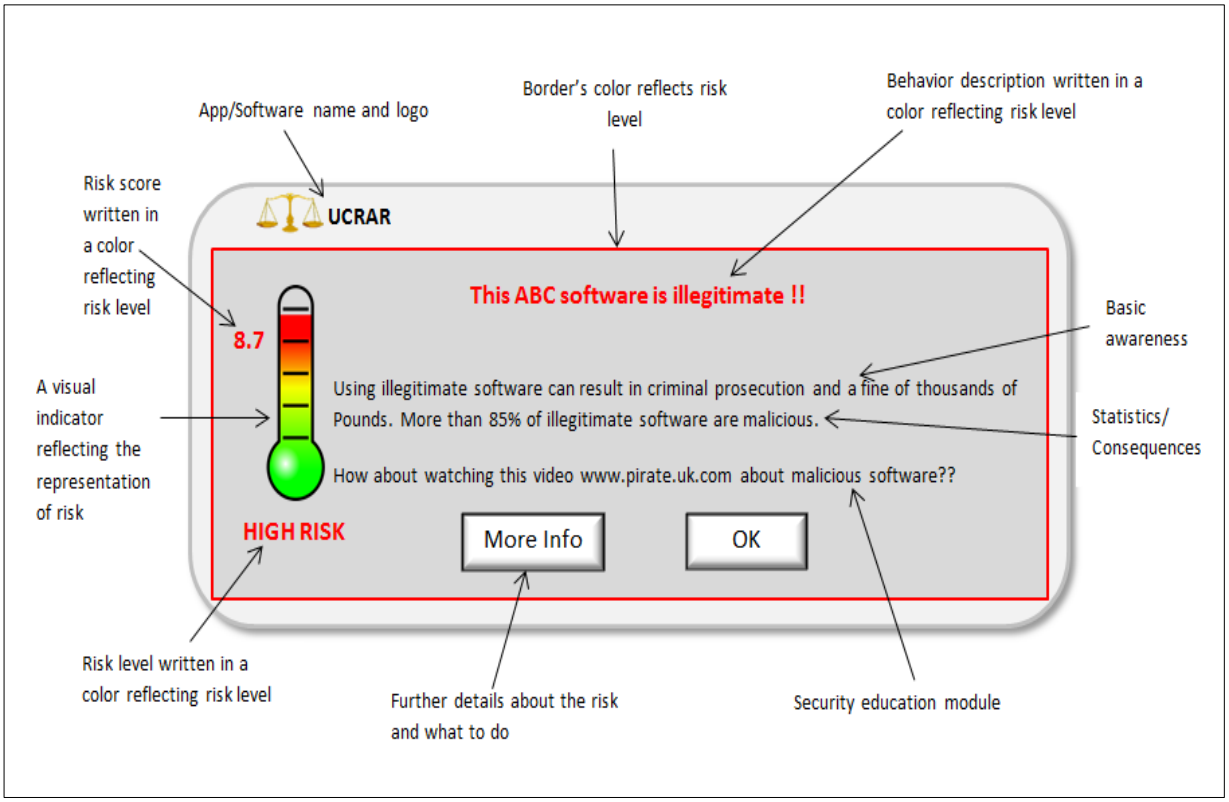

Figure 5.3: Suggested Design of an Alert

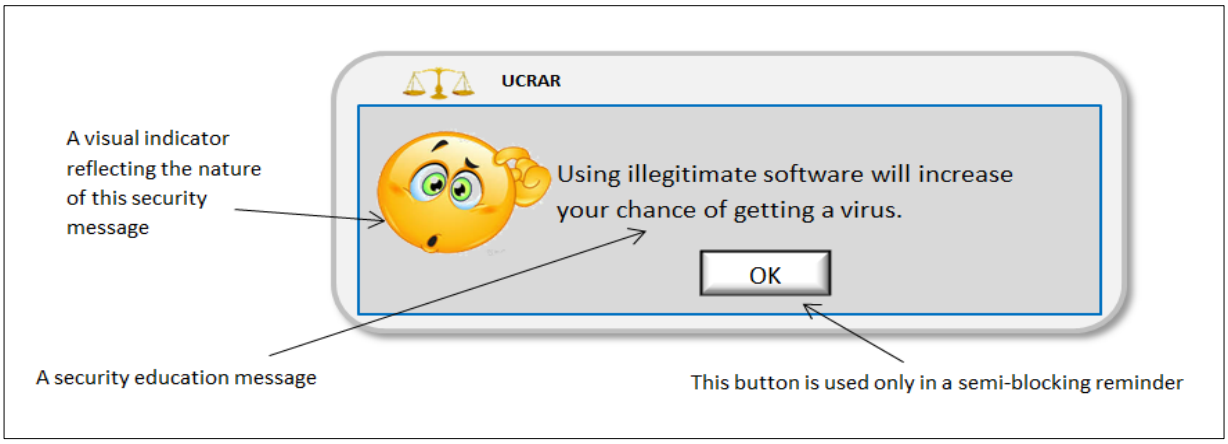

Figure 5.4: Suggested Design of a User's Behavior Reminder

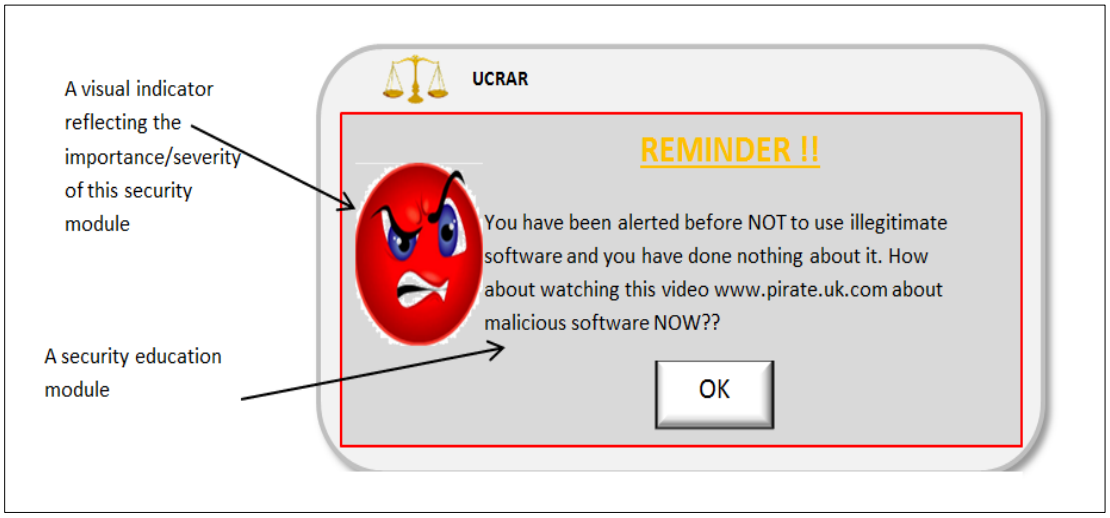

Figure 5.5: Suggested Design of a Security Education Module Reminder

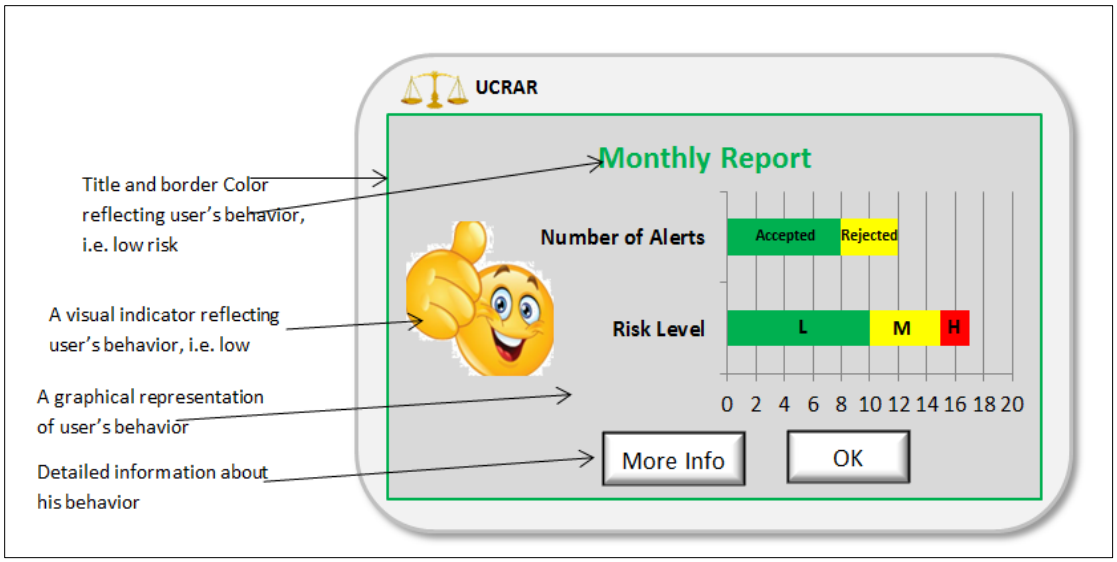

Figure 5.6: Suggested Design of a User's Behavior Report

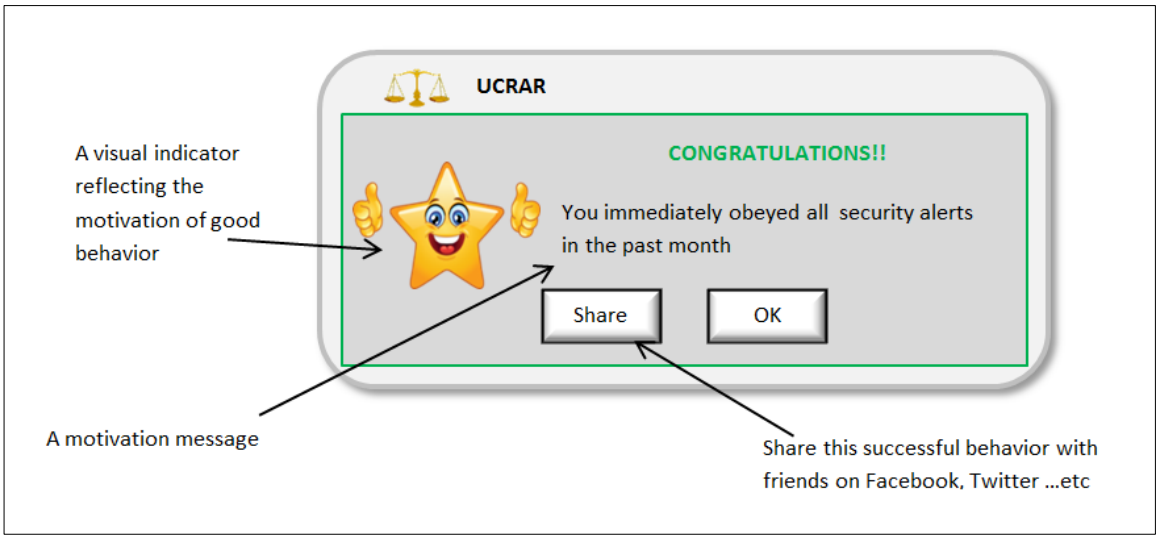

Figure 5.7: Suggested Design of a Motivation Alert

5.3.2.2 Historical Risk Register

All user's behaviors, whether secure or insecure, and information related to it are continuously stored in this register/database. Whenever a risk profile is received, it is compared with relevant historical risk data. The result of this comparison is used to determine the type/level of response. This will be stored as the following tuple:

Res-behavior= (*b-actual, date, response-num, module, u-action, risk-score, risk level*)

Where: *reponse-num* is the number of the response displayed to the user as shown in Figure 5.2. *Reponse-num* Є {0,1,2,3,4,5,6,7,8}. 0 is used to indicate no response issued, i.e. secure behavior

Module is to indicate the type of recommended security education module (if any) of either security **aw**areness or **tr**aining. *Module* Є {aw, tr, no}

u-action is user's behavior towards a given module if any, i.e. ignored, or obeyed.

U-action Є {i,o}

Additionally, this information will be used by the Security Response Manager when issuing a motivation alert, user's behavior report and to identify areas in which the user has mostly behaved *insecurely* and in need of further education.

5.3.2.3 Alerts, Reminders/Notifications, Awareness and Training

This targeted risk communication goes beyond passively notifying/warning users of security risks to act as a tool to educating and training the user on good behavior to make security informed decisions whilst displaying the security message. This is can be achieved through additional teaching/education in the user's preferred learning style such as gamification, video and podcast. Additionally, in three different response approaches , six response levels and further details as an option as explained earlier.

5.3.2.4 Internet-Based Body of Knowledge

To educate the user about security, a form of targeted security education (basic awareness, consequences, awareness module and training module) will be provided based on user's behavior focusing, mainly, on educating him of his risk taking behavior. This will be decided upon by searching an Internet based body of knowledge that is developed by a third party, or simply the Internet as a huge knowledge base for security information such that the required security information will be searched for, identified and located on the Internet. As the accuracy and

effectiveness of such provided info should be evaluated, the creation of such knowledge base and evaluation of retrieved security information are outside the scope of work of this research and could be part of future work.

Given the researcher's focus on proposing a user-centric model to assess user's behaviors, this research was not designed to propose and evaluate the best approach to communicate risk to the user. Actually, the suggested risk communication approach was used as means to show how the results of the risk assessment, i.e. risk profile, can be used to communicate and educate users about risks in a way that goes beyond the one message/one size fits all approach. It is anticipated that this suggested approach will give the users a better understanding of various security issues, threats and how to avoid them in an individualized way. It is believed that doing work in both components of the proposed UCRAR Framework is beyond the work of a single PhD. As such, a decision was made to focus on the Risk Assessment component and not to move forward in the Risk Communication component of UCRAR.

5.4 UCRAR's Operational Flow

To assess and communicate risk, the previously mentioned processes need to collaborate together. As user's behaviors are continuously and transparently monitored, the risk assessment process is triggered by the query request sent by the Automated User-behavior Monitor to the Good Behavior knowledge base. The Good Behavior Knowledge base will compare user's behavior against a set of behavior's related descriptors as described in Section 5.3.2 and sends the query result back to the Automated User-behavior Monitor. This result is sent to the User-centric Risk Estimator as a user-centric risk assessment request. Additionally, user and behavior information such as behavior type and whether it is an application or system related behavior are sent along with the assessment request. However, to reduce processing overhead, user information maybe cached into the User-centric Risk Estimator. Upon receiving this request, the User-centric Risk

Estimator will send an application information request to the Software/App Detector which is needed for the assessment process. After getting the result, user-centric assessment is performed based upon the received information and the user-centric risk assessment result is sent to the Risk Aggregator. Hence, the User-centric Risk Estimator assesses behavior's risks based on information received from both The Automated User-behavior Monitor and the Software/App Detector.

Meanwhile, the Software/App Detector will send information about the current software/application and Operating System to the System-based Risk Estimator. To assess user's end-to-end communication, if any, the System-based Risk Estimator will issue a network information request to the Network Estimator process. After receiving all device information, i.e. application, Operating System and Network Router software, a device information query is sent to the CVE/NVD knowledge base for vulnerability data. Hence, the System-based Risk Estimator assesses system's risks based on information collected from the Software/Application Detector, Network Estimator and CVE/NVD knowledge base. Subsequently to calculating the security score for each of device information, the system-based risk assessment is carried out and the result is sent to the Risk Aggregator process. Then, a final risk assessment is done by the Risk Aggregator. By combining both risk assessment results, user-centric and system-based, a final risk score is calculated and a resulting risk profile is generated and sent to the Security Response Manager as shown in Figure 5.8.

The risk communication process starts by the Security Response Manager receiving the risk profile and analyzing its data. Similar to the User-centric Estimator, user information maybe cached into the Security Response Manager. The Risk Evaluator sub-process of the Security Response Manager will first check the risk level of the behavior. If it is low, i.e. secure, then secure-response-behavior information will be sent immediately to the Historical Risk Register. Otherwise, it is sent to the Response Organizer sub-process which will send a behavior query to the

Historical Risk Register. Based on the query result, the Security Response Manager will decide upon the response. Before communicating the risk, a query is sent to the Internet-based Body of Knowledge for security education information related to the behavior. User's response to the risk communication is sent to the Historical Risk Register along with response-behavior information as in Figure 5.9.

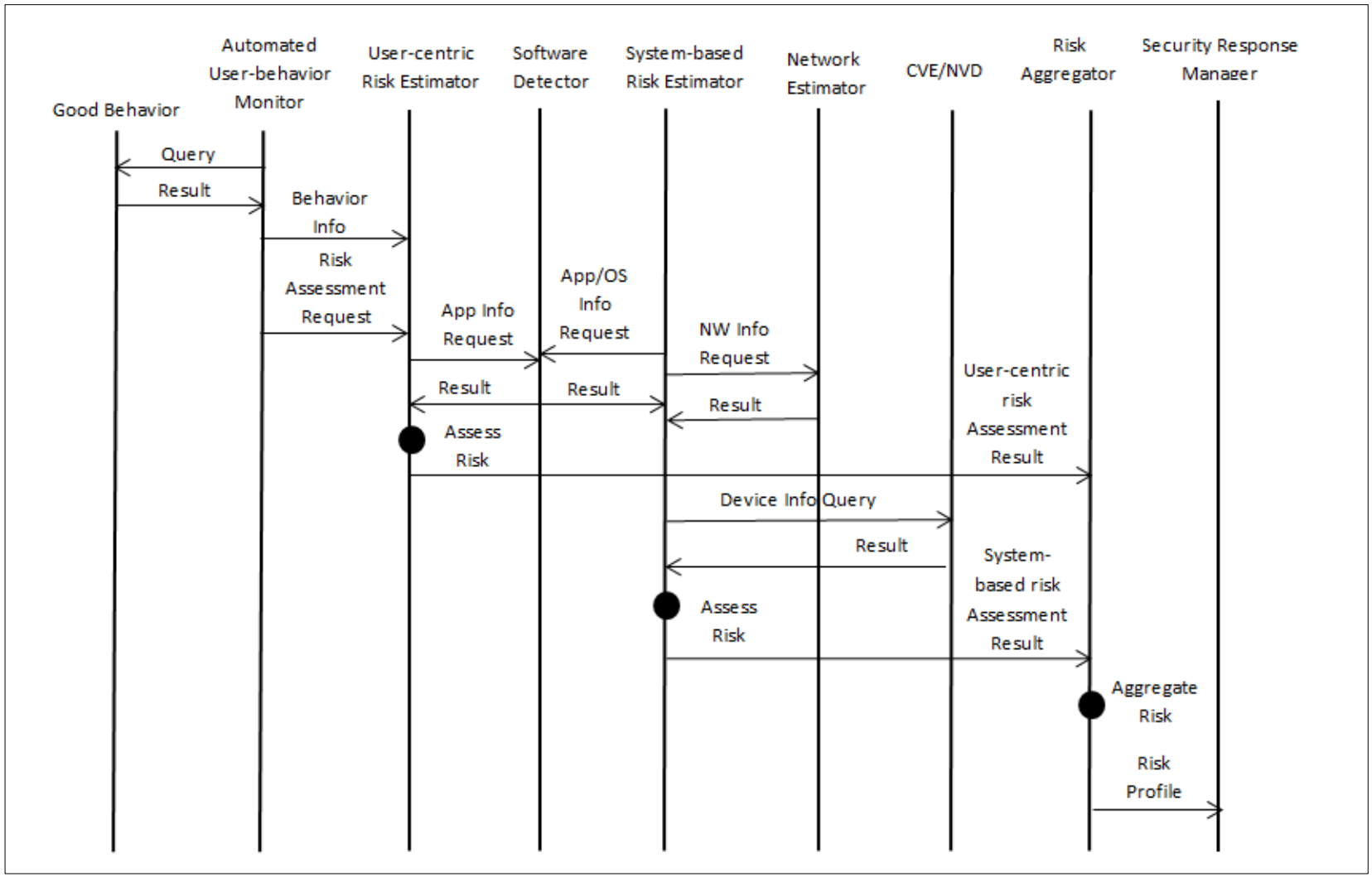

Figure 5.8: Operational Flow in The Risk Assessment Component

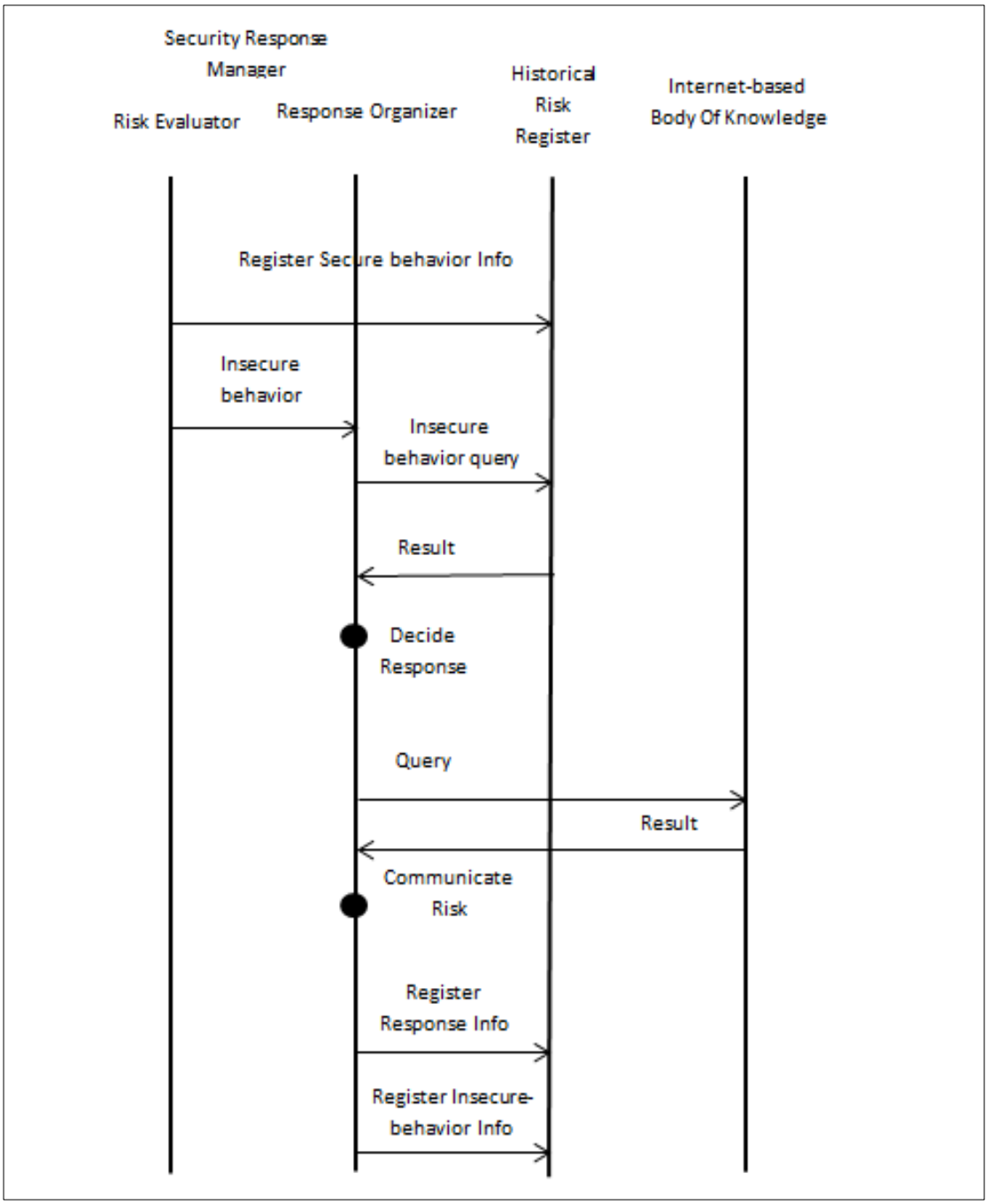

Figure 5.9: Operational Flow in The Risk Communication Component

To further explain how a response decision is made in this operational flow, a scenario is assumed of four different behaviors undertaken by a user in a time span of three months from 1-9-

2017 to 1-12-2017 as in Table 5.6. The user is assumed as a medium level service usage user. The response to his behavior is as described in section 5.3.2.1 and according to the response mechanism of Figure 5.2.

Behavior #	Behavior Name	Date	Risk score/level
1	Behavior A	1-9-2017	3.2 / L
2	Behavior B	5-9-2017	8.8 / H
3	Behavior C	12-9-2017	5.3 / M
4	Behavior B	13-9-2017	7.3 / H
5	Behavior D	20-9-2017	6.5 / M
6	Behavior C	5-10-2017	6 / M
7	Behavior D	6-10-2017	7.6 / H
8	Behavior B	20-10-2017	6.2 / M
9	Behavior C	25-11-2017	6.7 / M
10	Behavior D	1-12-2017	4.8 / M

Table 5.6: Response Scenario Behaviors

- **Behavior #1:**

  Risk level = Low, i.e. secure behavior. Thus, no alert issued and response-behavior-info is sent to Historical Risk Register.

- **Behavior #2:**

  Risk level = High, i.e. insecure behavior.

  Behavior was not seen before, i.e. first time. Thus, Response 2 is issued. User's response is recorded and sent to the Historical Risk Register along with response-behavior-info.

- **Behavior #3:**

  Risk level = Medium, i.e. insecure behavior.

  Behavior was not seen before, i.e. first time. Thus, Response 1 is issued. User's response is recorded and sent to the Historical Risk Register along with response-behavior-info.

- **Behavior #4:**

  Risk level = High, i.e. insecure behavior

  Behavior was seen before. Last seen 8 days ago, i.e. short time period.

Current risk score (7.3) < last time risk score (8.8). thus, Response 7 is issued. User's response is recorded and sent to the Historical Risk Register along with response-behavior-info.

- **Behavior #5:**

  Risk level = Medium, i.e. insecure behavior.

  Behavior was not seen before, i.e. first time. Thus, Response 1 is issued. User's response is recorded and sent to the Historical Risk Register along with response-behavior-info.

- **Behavior #6:**

  Risk level = Medium, i.e. insecure.

  Behavior was seen before. Last seen 24 days ago, i.e. medium time period.

  Current risk score (6) > last time risk score (5.3). Thus, Response 6 is issued. User's response is recorded and sent to the Historical Risk Register along with response-behavior-info.

- **Behavior #7:**

  Risk level = High, i.e. insecure behavior.

  Behavior was seen before. Last seen 17 days ago, i.e. short time period.

  Current risk score (7.6) > last time risk score (6.5). Thus, Response 8 is issued. User's response is recorded and sent to the Historical Risk Register along with response-behavior-info.

- **Behavior #8:**

  Risk level = Medium, i.e. insecure behavior.

  Behavior was seen before. Last seen 38 days ago, i.e. medium time period.

  Current risk score (6.0) < last time risk score (7.3). Thus, Response 5 is issued. User's response is recorded and sent to the Historical Risk Register along with response-behavior-info.

- **Behavior #9:**

  Risk level = Medium, i.e. insecure behavior.

  Behavior was seen before. Last seen 51 days ago, i.e. long time period.

  Current risk score (6.7) > last time risk score (6.2). Thus, Response 4 is issued. User's response is recorded and sent to the Historical Risk Register along with response-behavior-info.

- **Behavior #10:**

  Risk level = Medium, i.e. insecure behavior.

  Behavior was seen before. Last seen 55 days ago, i.e. long time period.

  Current risk score (7.6) > last time risk score (6.5). Thus, Response 3 is issued. User's response is recorded and sent to the Historical Risk Register along with response-behavior-info.

5.5 Conclusion

A novel framework that aims to assess, communicate and educate users about risks in a continuous, individualized and timely manner was proposed. This is accomplished by continuously and transparently monitoring his behaviors. The novelty of this proposed framework is that it attempts to assess user's risk-taking behaviors from both a user-centric and a system-based perspective to generate a final individualized risk score/level. However, in order to determine this risk score/level, novel Information Security Risk Assessment Models that assess risk on both the user and system levels and take into account user-centric factors among other factors as part of this assessment are required. These models need to be utilized within the functionality of the Risk Assessment component of the proposed UCRAR framework. Namely, the User-centric Risk Estimator, System-based Risk Estimator and the Risk Aggregator processes of the Risk Assessment Component.

Not limited to that, an individualized risk profile with user's risk data is created and used as means on how to best communicate risk to the user. Based on the analysis of user's behavior and other factors within the risk profile, a decision is made upon the best persuasive and individualized form of communicating/educating the user about his insecure behavior. Aside from the traditional approaches to risk communication such as the one message and one-size-fits-all approaches, responding to insecure behaviors goes beyond alerting the user of his insecure behavior to providing a level of security education. This is done in a gradual manner utilizing three different response approaches and six response levels.

Chapter 6 : A Novel Approach to Information Security Risk Assessment

6.1 Introduction

In order for the aforementioned UCRAR framework to operate, there needs to be a mechanism upon which risk is calculated and explicitly incorporates user interaction and user's behaviors in understanding risk. Having established that risk is changing within an application, there exists other sources of risk on the system level and that a number of different user-centric factors affect user's risk-taking behavior, the outstanding research question is how to calculate that risk. Therefore, based on Figure 5.1, three risk estimation models are proposed in this chapter to timely calculate risk apart from the traditional risk assessment formula where risk is calculated as

$$\text{Risk} = \text{Asset} \times \text{Threat} \times \text{Vulnerability}.$$

These models are namely, System-based Risk Estimation Model, User-centric Risk Estimation Model and the Aggregated Risk Estimation Model to be used by System-based Risk Estimator, User-centric Risk Estimator and the Risk Aggregator processes of UCRAR respectively.

As discussed in Chapter 2, various risk assessment techniques whether qualitative, quantitative or semi quantitative are given in (ISO 2009) that have been used in the literature to assess and analyze information security risks such as fault tree analysis, cause and effect analysis, Bayesian networks and decision trees (Alguliev et al. 2009; Imamverdiyev 2013; Pirzadeh and Jonsson 2011; Poolsappasit et al. 2011; Sadiq et al. 2010; Tamjidyamcholo et al. 2013; Tao et al. 2010). A matrix-based approach is a sound, tested, well documented and widely used approach amongst risk assessment methodologies (ISO 27005 2011). Therefore, in these proposed three models, the calculation of risks is on the basis of a risk matrix. A vulnerability-oriented approach (NIST 2012) where the method starts with the identification of a set of vulnerabilities is adopted as explained in

Section 5.3.1.7. Hence, some form of information source that can measure the criticality or vulnerability of software is needed. Currently, this could be done through the CVSS scoring algorithm. Thus, risk scoring will be based on the scoring system used by (Mell et al.,2007). Consequently, the generated risk scores of each model are quantitative numbers between 0 and 10, where 0..3.9 = low risk, 4..6.9 = medium risk and 7..10 = high risk.

In the rest of this chapter, the proposed system-based risk estimation model is discussed in section 2 followed by an explanation of the proposed user-centric risk estimation model. How the results of these proposed models are used to generate an aggregated risk profile using a proposed aggregated risk estimation model is demonstrated in section 4 followed by a conclusion in section 5.

6.2 System-based Risk Estimation Model

For the system-based risk assessment, a vulnerability-oriented approach will be used to assess and analyze security risks on the system level through the use of CVSS scoring algorithm. To calculate a software risk score/level, the System-based Risk Estimator process of UCRAR will check all installed software, router software and also platform information in terms of the used Operating System for known vulnerabilities. This is done by using knowledge bases such as NVD and CVE. Time is a critical factor in determining the severity of such vulnerabilities. Thus, the methodology proposed by (Wu and Wang 2011) will be used to calculate the risk score (0.. 10) of installed applications, *app-risk*, the used Operating System, *os-risk*, and router's software, *nw-risk*. However, this methodology is not definitive and the nature of the proposed model allows the use of any software risk scoring methodology.

As applications installed from illegitimate sources such as suspicious websites and non-legitimate app-markets or pirate software maybe malicious, thus, increasing the vulnerability to various attacks, the source name of the installed application, *install-name*, is used as a risk factor.

Since this risk factor is application-specific, then it will be added to the calculated *app-risk*. If the application was installed from an illegitimate source, then the final security score of the application, *app-risk*, is re-calculated as follows:

IF *install-name* = illegitimate THEN (1)
IF 0<= *app-risk* <= 3.9 THEN *app-risk* = 4 {increase app risk level from low to medium}
ELSE IF 4<= *app-risk* <=*6.9 THEN app-risk* = 7 {increase app risk level from medium to high}

There is an understanding that each of the application, router and operating system has a different impact on the overall system risk. As no evidence yet on the amount/percentage of impact each of these aspects has, weights are used. In practice, it could be quite difficult to understand how to set these weights. Indeed, future work will need to identify a mechanism in which this could be done more reliably. Whenever any evidence is found, the model is flexible enough to adopt to it. Therefore, the final system risk score, *system-risk*, is calculated as follows:

$$System\text{-}risk = App\_risk * w_{app} + OS\_risk * w_{os} + NW\_risk * w_{nw} / (w_{app}+w_{os}+w_{nw}) \quad (2)$$

where w_{app}, w_{os} and w_{nw} are subjective weights.

Thus, the resulting system risk score, s*ystem-risk,* is the is the quantitative system risk score where $0 \leq system\text{-}risk \leq 10$. Accordingly, the resulting system risk level is 0..3.9 Low, 4..6.9 Medium and 7..10 High.

6.3 User-Centric Risk Estimation Model

The findings of Chapter 4, demonstrated the impact of user-centric factors on users' risk taking behavior. This suggested that given a certain user behavior and different users, risk is not the same for all of them. As such, these user-centric factors will be considered as a risk factor when assessing risk on the user level. As threat against a certain application maybe increased due to user's insecure behavior, behaviors are assessed, resulting in a risk score/level, *behavior-score*, and used as a risk factor. Additionally, other risk factors that are behavior-related are considered such as the application importance, *app-score*, as detected by the Software Detector process and the

used communication channel. Consequently, assessing these user-centric and behavior-related risk factors will result in an individualized risk score/level, *behavior-risk*.

6.3.1 A Categorization of User's Behaviors

The first step in this proposed risk estimation model is to have a list of possible user's behaviors in order to understand what needs to be measured and quantified. Nevertheless, it is unrealistic to assume all possible user's behaviors especially with the existence of multiple platforms and the increasing number of applications on a yearly basis (Statista.com 2016). As such, when looking at mobile devices usage for example, a list of possible user's behaviors is as in Appendix B. For this purpose, applications were categorized into groups and an example application of each category was selected based upon its popularity, i.e. number of subscribers. Although this comprehensive list of behaviors is in the context of mobile devices, but it does not include any platform-specific behaviors and, accordingly, could be used as a starting point and generalized to any computing device.

However, to individually and continuously risk assess user's behaviors in near real-time could be time consuming. Most traditional risk assessment models (Karabacak and Sogukpinar 2005; Ledermuller and Clarke 2011; Theoharidou et. al 2012; Jing et. al 2014) rely on user input where users have to complete extensive questionnaires for example. This is not acceptable and may result in the user dumping or rejecting the application. Hence, the need to be particularly careful about placing input burdens/demands on the user is paramount. Therefore, to help automate this step, an approach has been taken to develop a structure upon which user's behaviors could be categorized as in Figure 6.1. In this suggested categorization, each behavior category has its own proposed risk assessment model. Namely, these behaviors could usefully be categorized as:

I. System/Device-related behaviors: These are stand-alone behaviors that are not application-specific. These could be classified as:

I.1 Device locking behaviors: These include the utilization (if any) of a device locking mechanism as means of authentication. Examples of such mechanisms are a password/pin lock, a face lock and a swipe pattern lock.

I.2 Connectivity: This refers to how the device accesses the Internet (i.e. network connections). These network connections/communication channels are either wired networks such as cellular network (3G/4G) or wireless communication such as public/private WiFi networks, Bluetooth and NFC. However, this is different from using a vulnerable router as when calculating system risk.

I.3 Settings behaviors: These are behaviors that are related to the settings options for system/device backups, system/device/applications update such as enabling auto-checking for updates and privacy options such as enabling location services.

I.4 Responding to security alerts: These include responding/rejecting various security alerts whether issued by UCRAR or by other applications.

II. Application-related behaviors: These are behaviors regarding the way the user is using the different processes (functionalities) within an application such as opening an email attachment within the Gmail application, posting on the Facebook wall and opening contacts in the Twitter application. These could be classified according to the nature of the behavior and the type of data accessed as follows:

II.1 Nature of behavior: from the application-related behaviors mentioned in Appendix B, they could be classified as:

II.1.1 Read behaviors: These are passive behaviors where there is no sharing of information with others. Examples of such behaviors are forecasting the weather, reading BBC news or services provided by HSBC.

II.1.2 Write behaviors: These are the behaviors where the user is sharing (exposing) information with others such as tweeting in Twitter, posting a photo in Facebook or writing a message in Whatsapp.

II.1.3 Settings behaviors: These are behaviors that are related to changing settings of an application such as turning on photo tagging in Twitter and "who can look me up" in Facebook.

II.1.4 Authentication behaviors: These are behaviors related to the signing in to an application/service (if any) using an authentication mechanism, i.e. passwords.

II.2 Type of data accessed: Data is classified according to the risk and impact on user's CIA and privacy when this data is modified or disclosed. Consequently, data could be either:

II.2.1 Private: Examples of such data are email contacts and personal photos of the user.

II.2.2 Public: Examples of such data are products on sale in Amazon and weather news on BBC.

These two types of data are, mainly, related to the read/write behaviors, i.e. read-private-data, read-public-data, write-private-data and write-public-data.

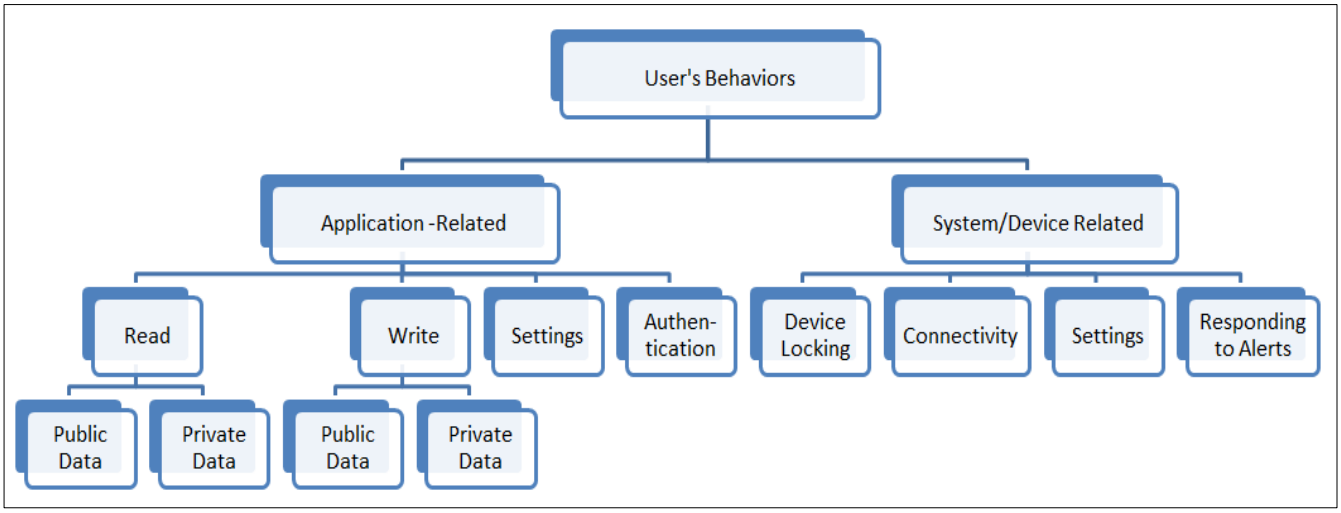

Figure 6.1: A Suggested Categorization of User's Behaviors

As an example of the generalizability and applicability of this proposed categorization and to benefit from empirical data, a mapping of behaviors mentioned in the users' survey of Chapter 4 to the categorization of user's behaviors is as given in Table 6.1.

Categorization of User's Behaviors				Behaviors of Users' Survey (Chapter 4)
User's Behaviors	Application-related	Authentication		▪ Changing of passwords ▪ Using the same password for multiple sensitive accounts
		Settings		▪ Disable Ant-virus software because it was slowing my device ▪ Logging off from online systems
		Read	Private	▪ Clicking on links/attachments in emails from unknown senders without checking ▪ Clicking on links/attachments in emails from friends without checking
			Public	-------
		Write	Private	▪ Storing of passwords ▪ Deleting suspicious emails ▪ Using encrypted USBs when transferring data ▪ Encrypting sensitive information ▪ Using pirate software ▪ Allowing web browsers to remember my passwords
			Public	▪ Downloading files from unknown/suspicious websites ▪ Forwarding chain emails
	System/device-related	Device locking		▪ I lock my workstation when away ▪ I use a password for my home PC
		Connectivity		▪ Connecting to public WiFis such as in shopping malls and coffee shops ▪ Disabling of wireless services such as WiFi and Bluetooth when not used ▪ Using an anonimying proxy ▪ Using a TOR network ▪ Using a VPN
		Settings		▪ Keeping Anti-virus software up-to-date ▪ Scanning of USBs before using them ▪ Backing up of data on a regular basis ▪ Installing of patches
		Responding to alerts		▪ Canceling/postponing a security related update ▪ Opening a document despite security warnings

Table 6.1: A Mapping of User's Survey Behaviors of Chapter 4 to The Suggested User's Behaviors Categories

When looking at these types of behaviors, two different situations were identified especially in the case of authentication and connectivity behaviors. To differentiate them, they are denoted as primary and secondary behaviors. A primary behavior is when the behavior is a stand-alone behavior and it is assessed independently of any other behavior. Whereas a secondary behavior is when the behavior assessment result is combined with the assessment of another behavior as explained in the next sections.

6.3.2 Application-related Behaviors

A risk assessment model is proposed for each application-related behavior category as follows:

- **Authentication behaviors**, two situations are identified:

A. When the authentication behavior itself is assessed independently of any other behaviors such as signing in to Twitter account or using the same password for multiple sensitive accounts. Hence, the authentication behavior is the primary behavior.

B. When this behavior relates to an application/service that requires authentication and its assessment result is combined with the assessment of another behavior such as writing an email with personal details using Gmail and the email password is weak. Hence, the authentication behavior is not the primary assessed behavior but a secondary behavior and its risk assessment is combined with the primary behavior.

In both situations, the same approach is applied to assessing its risk. The used password is assessed, first, for its hygiene against a predefined rule-set of 0=low, 1=medium and 2=high. Passwords are checked for several attributes such as its length, password reuse, how old the password is and the utilization of uppercase, lowercase, numbers and special characters. An authentication risk matrix is generated for each attribute as in Matrix1. Each password attribute is assessed as Low, Medium or High and mapped into Matrix 1.

		Password Attribute		
		Low	Medium	High
app-score	0	0	1	2
	1	1	2	3
	2	2	3	4
	3	3	4	5
	4	4	5	6

Matrix 1: Authentication Matrix, *auth-score*

Second, each application will be mapped into its corresponding category and, consequently, assigned its importance level, *app-score*. This *app-score* was generated by the Software Detector based on user input and has values 0= very low, 1= Low, 2= Medium, 3= High and 4= Very High. Finally, based on the "worst case scenario" principle (Theoharidou et al. 2012), the maximum value resulting from the above risk matrix is used. Hence, an authentication behavioral risk score, *auth-score*, will be generated as

$$auth\text{-}score = \text{MAX(attributes)} \quad (3)$$

If authentication behavior is assessed independently of any other behaviors, i.e. primary behavior, then the resulting *auth-score* is reassessed based upon the significance correlation risk factor (if any) as explained in section 6.3.3. However, as all scores used in the risk assessment are from 0 to 10, the resulting *auth-score* will be normalized. The resulting risk score is the behavioral risk score, *behavior-risk*

$$behavior\text{-}risk = \text{normalize (significant (}auth\text{-}score\text{))} \quad (4)$$

- **Application-related settings behaviors**, risk is assessed for this category of behaviors such that If the setting is disabled as in behaviors of "Disabling Anti-Virus software" and "Not logging off from online systems", then risk is high. Then, the related application will be mapped into its corresponding category and, consequently, assigned its importance level, *app-score* as generated by the Software Detector. The assessment of behavioral score, *behavior-score,* depends on *app-score* as in Matrix 2. Thus,

IF *app-score* = 0 THEN *behavior-score = 2* (5)
ELSE IF IF *app-score* = 1 THEN *behavior-score = 3*
ELSE IF *app-score* = 2 THEN *behavior-score = 4*
ELSE IF *app-score* = 3 THEN *behavior-score = 5*
ELSE IF *app-score* = 4 THEN *behavior-score = 6*

The resulting *behavior-score* is reassessed based on the significance correlation risk factor (if any). As all scores used in the risk assessment are from 0 to 10, then the resulting *behavior-score* will be normalized. Finally, the resulting risk score is the behavioral risk score, *behavior-risk*.

behavior-risk = normalize (significant (*behavior-score*)) (6)

- **Application-related behaviors of Read and Write**, each behavior depending on its nature and data accessed has its own consequences. As the impact of consequences of various user behaviors generate different risk levels within an application where the nature of the behavior may escalate or deescalate the risk level of an application. This is evident as a "read" behavior has a different risk level than a "write" behavior. Furthermore, the data type accessed by the behavior plays a role in the risk assessment whereas reading the weather has different impact consequences than reading a bank's account balance. Similarly, sharing (writing) a link on BBC News has different impact consequences from posting (writing) a family photo on Facebook. However, reading public data such as browsing products in Amazon, reading the weather forecast or searching Google maps might have no potential consequences on the user, hence no risk.

  Adopted from CRAMM (Yazaar 2011), seven impact consequences are identified:

  - Impact of Disruption (D)
  - Impact on Personal Privacy (P)
  - Impact of Data Corruption (DC)
  - Impact of Embarrassment (E)
  - Financial Lost (F)

- Legal Liability (LL)
- Impact on Personal Safety (S)

As it is hard to assess this from one user to another due to different user-centric factors and to provide a fine-grained valuation that reduces the burden on the user in terms of user input, the potential consequences will be assessed and assigned for each behavior category. Then, each behavior will be mapped into its corresponding category. For simplicity, potential consequences are rated as **0-Low (L)**, **1-Medium (M)** and **2-High (H)**. An example of the suggested behavior consequences rating is as in Table 6.2.

	Suggested Consequences						
Behavior Category	**E**	**F**	**P**	**DC**	**LL**	**S**	**D**
Read-private-data	2 (H)	0 (L)	2 (H)	2 (H)	0 (L)	0 (L)	1 (M)
Write-private-data	1 (M)	2 (H)	2 (H)	2 (H)	1 (M)	0 (L)	0 (L)
Write-public-data	1 (M)	0 (L)	1 (M)	1 (M)	0 (L)	0 (L)	1 (M)

Table 6.2: An Example of Suggested Behavior Consequences

Each application will be mapped into its corresponding category and, consequently, assigned its importance level, *app-score*. This *app-score* was generated by the Software Detector based on user input and has values 0= very low, 1= Low, 2= Medium, 3= High and 4= Very High. A risk matrix will be generated for each consequence as in Matrix 2.

		Consequence		
		Low	Medium	High
app-score	0	0	1	2
	1	1	2	3
	2	2	3	4
	3	3	4	5
	4	4	5	6

Matrix 2 : Behavior Matrix , *behavior-score*

The first step in assessing the behavioral risk score is by identifying the *app-score* and the behavior's nature, type, accessed data-type, and consequences. Second, based on the "worst case scenario" principle (Theoharidou et al. 2012), the maximum value resulting from the above risk matrix is used. Hence, a behavioral risk score, *behavior-score*, will be generated as

$$behavior\text{-}score = \text{MAX(consequences)} \quad (7)$$

Additionally, both the used password and communication channel are assessed as additional risk factors, i.e. *auth-score* and *connect-score*, as explained earlier. Given that the disclosure or modification of private data in a private Facebook account, for example, has a lower risk level than in a public account, a pre-set score is assigned for each account type as:

IF account-type = Public THEN *account-type-score* = 2 (8)
ELSE IF account-type = Private THEN *account-type-score* = 1

To calculate *behavior-risk*, two situations are identified:

- If the assessed behavior is significantly correlated with a user-centric factor, then the resulting *behavior-score* is recalculated based on the significance correlation risk factor. Finally,

$$behavior\text{-}risk = \text{AVG}(behavior\text{-}score, auth\text{-}score, connect\text{-}score) + account\text{-}type\text{-}score \quad (9)$$

- If the assessed behavior is not correlated with a user-centric factor, then behavior-risk is calculated as in (9). However, as all scores used in the risks calculations are from 0 to 10, the resulting *behavior-risk* will be normalized.

Regardless of the application-related behavior category, the resulting behavior risk score, *behavior-risk,* is the quantitative behavior risk score where $0 \leq behavior\text{-}risk \leq 10$. Accordingly, the resulting behavioral risk levels are 0..3.9 low, 4..6.9 medium and 7..10 high.

6.3.3 The Significance Correlation Risk Factor

The novelty of this risk assessment scheme is that a different risk profile is created for the same behavior given a number of users. From the findings of Chapter 4, it was found that the risk score/level of a behavior may be positively or negatively affected by certain user-centric factor

such as personality trait, age and IT proficiency. Thus, the significance of the correlation between a user's behavior and user's-centric factors (if any) is used as a risk factor to reassess the behavioral risk score, *behavior-score*. Although one or more user-centric factors were found to be significantly correlated with a behavior, only the user-centric factor with the most significant correlation is used in the proposed risk assessment models as a risk factor. A number of user-centric factors have two possibilities/values (low and high) such as personality trait, IT proficiency and gender whereas service usage and age have three possibilities/values (low, medium and high).

However, when considering the significance correlation risk factor, two situations are identified, namely, the significance correlation risk factor for application-related behaviors and the significance correlation risk factor for system/device-related behaviors.

I. The Significance Correlation Risk Factor for Application-related behaviors:

The significance of a correlation implies that due to certain user-centric factors values, the likelihood of a security threat is either decreased or increased. Asset value is equivalent to the application's importance level from the user's perspective whereas how easy a security breach may occur depends on the type of user's behavior. Hence, the following matrix is adopted from (ISO 27005 2011) where user-centric factor value, *behavior-score* and *app-score* are used instead of threat likelihood, ease of exploitation and asset value respectively in the original matrix. Thus, the significance matrix is as in Matrix 3.

User-centric factor Value		Low			Medium			High		
behavior-score		L	M	H	L	M	H	L	M	H
App-score	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Matrix 3: Significance Correlation Matrix

The proposed methodology is as follows:

1. Determine the value of the user-centric factor, i.e. high, medium or low.
2. Determine the related *app-score,* i.e 0..4
3. Determine the *behavior-score* resulting from Matrix 1. This is a quantitative value between 0 and 6 where it will be mapped as 0..2 = low risk, 3 = medium risk and 4..6 = high risk.
4. IF –ve correlation THEN (10)
   IF user-centric factor = high THEN {decrease the risk }
   An opposite mapping will occur by mapping the user-centric factor to low level. Based on *behavior-score* and *app-score* a new risk score/ level will be assigned to *behavior-score.*
   ELSE IF user-centric factor = low THEN {increase the risk }
   An opposite mapping will occur by mapping the user-centric factor to high level. Based on *behavior-score* and *app-score* a new risk score/level will be assigned to *behavior-score.*
   ELSE IF user-centric factor = medium THEN
   The user-centric factor is mapped to medium level. Based on *behavior-score* and *app-score* a new risk score/level will be assigned to *behavior-score.*
5. IF +ve correlation THEN (11)

   IF user-centric factor = high THEN {increase the risk}
   The user-centric factor is mapped to high level. Based on *behavior-score* and *app-score* a new risk score/level will be assigned to *behavior-score.*
   ELSE IF user-centric factor = low THEN {decrease the risk }
   The user-centric factor is mapped to low level. Based on *behavior-score* and *app-score* a new risk score/level will be assigned to *behavior-score.*
   ELSE IF user-centric factor = medium THEN
   The user-centric factor is mapped to medium level. Based on *behavior-score* and *app-score* a new risk level will be assigned to *behavior-score.*

II. The Significance Correlation Risk Factor for System/Device-related behaviors:

As these are not specific to a certain application, the proposed methodology is as follows:

1. Determine the value of the user-centric factor, i.e. high, medium or low.
2. Determine the *behavior-score*.

3. IF –ve correlation THEN (12)
   IF user-centric factor = high THEN {decrease the risk }
   behavior-score = *behavior-score* - 1
   ELSE IF user-centric factor = low THEN {increase the risk }
   behavior-score = *behavior-score* + 1
   ELSE IF user-centric factor = medium THEN
   Neither increase nor decrease the risk score.

4. IF +ve correlation THEN (13)

   IF user-centric factor = high THEN {increase the risk }
   behavior-score = *behavior-score* +1
   ELSE IF user-centric factor = low THEN {decrease the risk score}
   behavior-score = *behavior-score* - 1
   ELSE IF user-centric factor = medium THEN
   Neither increase nor decrease the risk score

6.3.4 System/Device-Related Behaviors

A risk assessment model is proposed for each system/device-related behavior category as follows:

- **Connectivity behaviors**, as there is no 100% safe communication channel, and given that a range of communication channels could be used to connect a computing device to the Internet, a pre-set risk level will be assigned to each channel. Apart from the use of a VPN, this risk level will be based on the security measures that are utilized for data transmission by the communication channel (Community Norton.com 2017). Therefore,

  - **Wired private networks and Cellular networks** (3G/4G), they normally contain provisioning regarding data privacy that protect the user better than WiFi networks. Although there is a probability of eavesdropping but the connection is encrypted and the used hardware is harder to obtain and more expensive than for WiFi eavesdropping. Thus, data sent over the cellular network is encrypted and considered to have the lowest risk of exposure.
  - **WiFi**, the risk level depends on the connected network as WiFi Protected Access, WPA, is considered to be more secure than Wired Equivalent Privacy, WEP. Usually, public Wifi

found in coffeeshops, shopping malls …etc transmit data unencrypted, thus resulting in higher vulnerability to security threats. However, a private WiFi at homes and offices utilizes data encryption and password-protected access making them safer than public WiFi and, consequently, introducing a medium risk level.

- **Bluetooth** connectivity, encrypted data is exchanged between devices over short distances (less than 10 meters). Paired devices can communicate only with user's consent. This pairing requires an authentication mechanism ensuring that a malicious connection is not possible without victims knowledge and acceptance. Once paired, this authentication is no longer required for future connections. However, security concerns arise when this trusted device is compromised. As a result, enabling this connectivity has a medium risk level especially when device is "discoverable", whether used for transmitting data or not.
- Similar to Bluetooth, Near Field Communication **NFC** is another form of two-way wireless communication between devices except that devices have to be in near proximity, 4 cm. Unfortunately, this technology does not offer built-in security measures. Given NFC ease of use where data is transferred by bumping two devices and lack of authentication, a hacker can easily manipulate data by being in near proximity. Knowing that NFC is sensitive to direction where a slight directional movement will disrupt the signal, a medium risk level is assigned to this kind of connectivity.

Nevertheless, connectivity risks are either assessed as:

A. A stand-alone system/device-related behavior, such as not turning off Bluetooth when it is not used. In this case, the behavior is the primary behavior and a predefined risk level as explained above is assigned to the used communication channel. For each risk level, an average risk score is assigned as 2, 5.5 and 8.5 for risk levels of low, medium and high respectively to generate *connect-score*. Hence, two situations are considered:

A.1 If the assessment is done only for the used communication channel such as the behavior of "connecting to a public WiFi network", then the resulting *connect-score* is reassessed based on the significance correlation risk factor (if any).

A.2 If time and status of connection is to be considered in the assessment such as in the behavior " Did not Disable connection", then if the connection is idle for a time period T, the resulting *connect-score* is reassessed based on the significance correlation risk factor (if any).

In both situations, the resulting risk score is the behavioral risk score, *behavior-risk*.

B. Combined with the assessment of other user's behaviors when used for means of transferring data, i.e. secondary behavior. Thus, a risk matrix is generated for the connectivity behavior, *connect-score*, as in Matrix 4.

		Connectivity		
		Low e.g. (3G/4G)	Medium e.g. (Bluetooth, NFC and Private WiFi)	High e.g. (Public WiFi)
app-score	0	0	1	2
	1	1	2	3
	2	2	3	4
	3	3	4	5
	4	4	5	6

Matrix 4: Connectivity Matrix , *connect-score*

Risks of the connectivity behavior are assessed by mapping the used communication channel's pre-assigned risk level with the related *app-score* to generate a *connect-score*.

- **Responding to alerts behaviors**, risk is assessed for these behaviors as stand-alone behaviors regardless of application importance, *app-score*. If an alert is ignored/no action taken by the user, then risk is high and an averaging approach is used to calculate *behavior-score*. This is by adding the values at both ends of the level's scale, i.e. high risk level has a risk score between 7 and 10, and dividing it by 2 as:

$$behavior\text{-}score = (7 + 10)/2 = 8.5 \quad (14)$$

The resulting *behavior-score* is recalculated based on the significance correlation risk factor (if any) resulting in *behavior-risk*.

If an alert is specific to a certain application such as in the behavior "Cancel/postpone a security related update", then the vulnerability score of the application as calculated by (Wu and Wang 2011) is additionally displayed to the user. However, the number of ignored alerts is calculated over a certain time period T. When it exceeds a certain threshold, awareness is enforced.

- **Settings behaviors**, risk is assessed such that If setting is disabled, then risk is high and

$$behavior\text{-}score = (7 + 10)/2 = 8.5$$

For the special cases of behaviors related to backups and updates, if setting is enabled but an old backup or out of date application/OS is detected, then risk is medium and

$$behavior\text{-}score = (4 + 6.9)/2 = 5.5 \quad (15)$$

The resulting *behavior-score* is recalculated based on the significance correlation risk factor (if any) resulting in *behavior-risk*.

- **Device locking behaviors**, risk is not only assessed if such control is utilized or not, but also the degree it complies to good authentication behavior such as password hygiene. Opposed to other user's behaviors, the consequences of this behavior are related to physical threats only, i.e. device lost or stolen. Thus, this particular behavior could be considered as a stand-alone behavior and its risk assessment is done individually and not combined with the assessment of other user's behaviors. Hence, risk is assessed such that:
    - If no lock is used, then risk is high and *behavior-score* is assessed as in (14)

- If device lock (PIN) is used, then it is assessed for its hygiene using Matrix 5. The suggested PIN hygiene attributes are reuse, old, same number and predictable numbers. By mapping these risk levels in Matrix 5,

$$behavior\text{-}score = \text{MAX (PIN attributes)} \qquad (16)$$

	PIN Attributes											
	Reuse			Old			Same Number			Predictable numbers		
	L	M	H	L	M	H	L	M	H	L	M	H
Consequences	0	4	7	0	4	7	0	4	7	0	4	7

Matrix 5: PIN Assessment Matrix

The resulting *behavior-score* is recalculated based on the significance correlation risk factor (if any) resulting in *behavior-risk*

Regardless of system/device-related behavior category, the resulting behavior risk score, *behavior-risk,* is the quantitative behavior risk score where $0 \leq behavior\text{-}risk \leq 10$. Accordingly, the resulting behavioral risk level are 0..3.9 Low, 4..6.9 Medium and 7..10 High.

6.4 Aggregated Risk Estimation Model

To calculate the final risk score/level, *overall-risk*, an aggregated risk estimation model is required to assess the results of both user-centric and system-based assessment. Hence the following model is proposed and to be used by the Risk Aggregator process:

I. For Application-related behaviors: As this model was proposed, but within its scope and what we are trying to achieve, it has been recognized that it could be done in a variety of different approaches when assessing the final risk score/level, *overall-risk for* application-related behaviors. For example, a matrix-based approach could be used where all risk scores are rounded, i.e. 3.5 = 4. Similarly, an averaging approach could be used by simply adding *behavior-risk* and *system-risk* then dividing the result by 2. The proposed model for aggregating the user-centric risk score, *behavior-risk*, and the system-based risk score, *system-risk*, is

$$Overall\text{-}risk = (behavior\text{-}risk * w_{br}) + (system\text{-}risk * w_{sr}) \quad (17)$$

Where w_{br} and w_{sr} are subjective weights

Unfortunately, there is no evidence yet on the impact *behavior-risk* and *system-risk* or suggest the proportion of impact each of them have on the final risk score/level, *overall-risk*, therefore, weights are used. However, the proposed model allows for a variety of ways such that whenever future research is available regarding this proportion, the proposed model could easily adopt to it. If there is no information to suggest any other alternative, weights are set equally to 0.5.

II. For system/device-related behaviors: As a vulnerable application is not considered, arguably, as a threat source when assessing risks of system/device-related behaviors such as in not utilizing a device lock or in connecting to a public WiFi network. Moreover, the threat is in the behavior itself as a stand-alone behavior regardless of compound risks. Thus, *overall-risk* for system/device related behaviors is the same as the behavior risk score as

$$Overall\text{-}risk = behavior\text{-}risk \quad (18)$$

In both cases, the resulting final risk score, *overall-risk,* is the quantitative final risk score where $0 \leq overall\text{-}risk \leq 10$. Accordingly, the resulting final risk level are 0..3.9 low, 4..6.9 medium and 7..10 high.

Detailed worked examples of how these proposed mechanisms work are explained in the next chapter, section 7.3.2.

6.5 Conclusion

As variations in user-centric and behavior-related factors resulted in different risk scores/levels for the same behavior, an approach to a multi-platform risk assessment that considers these variations in near real time is needed. Hence, having a list of possible user's behaviors is the first

step in this approach. However, it is unrealistic to neither assume all possible user's behaviors nor assess each of them independently. Therefore, a categorization of user's behaviors is proposed. For each behavior category, a novel risk estimation model is proposed resulting in an individualized risk profile. Motivated by findings from Chapter 4, the significant correlation risk factor has been used in the proposed models when assessing risk either for application-related or system/device-related behaviors. These proposed multi-platform risk estimation models are an attempt to assess risks for users aside from the traditional approach. Nevertheless, the feasibility and applicability of such models need to be investigated and assessed.

Chapter 7 : An Evaluation of The Model for User-centric Information Security Risk Assessment

7.1 Introduction

As identified in Chapter 5, the proposed Model for User-centric Risk Assessment and Response, UCRAR, incorporates both risk assessment and risk communication. The focus of this research and this evaluation will be on the Risk Assessment component rather than the Risk Communication component. From the findings of Chapters 1-4, it has been found that risk cannot be treated the same for all users. Being that there are factors about risk that have been identified and quantified, a user-centric Information Security Risk Assessment Model is proposed where risk is assessed independently for each user using a number of proposed risk estimation models. The resulting risk scores/levels from those models will enable other processes of UCRAR, the Security Response Manager for example, to take that information and act accordingly.

Given that the proposed risk estimation models are dependent upon a variety of factors, whether user-centric such as IT proficiency and personality traits, or behavioral-related such as the used communication medium and authentication hygiene, the aim is to:

1) Evaluate the effectiveness and feasibility of the proposed model.
2) Examine the nature of the proposed risk assessment model and how it works.

Therefore, the following research questions are asked:

RQ1: What is the impact of a user-centric factor *x* on the model?

RQ2: What is the impact of a behavioral-related factor *y* on the model?

RQ3: Given a number of different users with different characteristics and behaviors, how does the model work?

This chapter is structured as follows: the evaluation methodology is described in the next section followed by analysis of the results in section 3. Section 4 discusses the results of the proposed models followed by a conclusion in section 5.

7.2 Methodology

To obtain meaningful answers to the proposed research questions, three non-user based experiments are done. However, a number of assumptions have to be made at first for Experiments I and II where some variables need to be controlled and the others varied to understand their impact.

Experiment I:

I.1 For a user-centric factor *x*, different possible categories are assumed such as 18-30 years, 31-50 years and 51+ years for the age factor and high conscientiousness and low conscientiousness for conscientiousness personality trait factor.

I.2 For a certain user behavior, an average risk score representing each risk level is assumed for all behavioral-related factors such as risk scores of 2, 5.5 and 8.5 to represent risk levels of low, medium and high respectively.

I.3 The model is applied and risk is calculated.

I.4 Results are analyzed to understand what change in the output, i.e. the resulting risk scores/levels, is obtained as a consequence of the change in input.

Experiment II:

II.1 For the same user-centric factor *x* as in Experiment I, different possible categories are assumed such as 18-30 years, 31-50 years and 51+ years for the age factor and high conscientiousness and low conscientiousness for conscientiousness personality trait factor.

II.2 For the same user behavior as in Experiment I, an average risk score representing each risk level is assumed for a behavioral-related factor *y* while other behavioral related factors are assumed the other risk scores/levels. For example, if the behavioral-related factor of authentication thru *auth-score* variable is assumed as low risk with risk score of 2, then other

behavioral-related factors are assumed medium and high with risk scores of 5.5 and 8.5 respectively.

II.3 The model is applied and risk is calculated.

II.4 Results are analyzed to understand what change in the output, i.e. the resulting risk scores/levels, is obtained as a consequence of the change in behavioral-related factor *y*.

Experiment III (Scenario-based Simulation):

To evaluate the model, there exists a number of challenges in implementing the proposed model on real users and within a real environment. The need to develop the required controls to do the process of user monitoring and the development of several knowledge bases such as the community-based risk data are examples of such challenges. Furthermore, this research is done by a single researcher with time constraints. Although different approaches could be taken to evaluate the model, the most complete and comprehensive approach that will enable a comprehensive analysis of the model appeared to be a simulation-based approach. In this approach, a number of users with different risk profiles across the spectrum will be replicated. Hence, in order to do a walkthrough of the proposed model and understand, in a categorized fashion, how different users are impacted by risk, a scenario-based simulation based upon a variety of users' profiles from one end to the other is designed considering the following:

1) All possible user-centric factors permutations for different users.
2) Based on findings of Chapter 4, two users with user-centric factors representing the two extremes of low and high risk profiles are assumed (users D and E).
3) Behaviors included in the scenario reflects examples of each behavior type from the suggested categorization of user's behaviors as in Figure 6.1 to understand the nature of how they impact the risk score/level.

4) Behaviors selected demonstrate the difference between the resulting risk scores/levels of behaviors that were found to be most significantly correlated with a certain user-centric factor and those that were not (Behavior 6).
5) Varying *app-scores* with low, medium, high and very high importance are assumed.

The experiment, i.e. scenario-based simulation, is done as follows:

III.1 The scenario is assumed.

III.2 A variety of users with different user-centric factors are assumed.

III.3 The model is applied and risk is calculated.

III.4 Results are analyzed to understand how different users are impacted by risk and if resulting risk scores/levels reflect trends and patterns observed in Experiments I and II.

Together, all of these experiments will give an understanding of what this model is going to do, how it works and the impact of the identified factors/behaviors have on the overall-risk.

7.3 Results

In order to perform these non-user based experiments, a number of assumptions have to be made at first. Then, the proposed model is applied and its performance is analyzed accordingly.

7.3.1 User-centric VS. Behavioral-related Analysis

For Experiments I and II, conscientiousness personality trait and the application-related behavior of write public data thru the behavior " Downloading files from suspicious/unknown websites" are selected as examples of a user-centric factor and a user behavior respectively. Based on findings of Chapter 4, this user behavior has a significant negative correlation with the mentioned user-centric factor. The impact of authentication hygiene thru the variable *auth-score* is selected as a behavioral-related factor. The type of this behavior, according to the suggested categorization of user's behaviors as in Figure 6.1, is an application-related write public data behavior where the proposed risk estimation model is as follows:

app-behavior-risk[1]=AVG(*behavior-score*, *auth-score*, *connect-score*)+*account-type-score*

The final risk score/level, *Overall-risk* = (*app-behavior-risk** W_{br})+ (*system-risk* *W_{sr})
where $W_{br=} W_{sr =}$ 0.5.

From Table 6.2, the suggested consequences of this behavior are

E = 1 (M), F = 0 (L), P = 1 (M), DC = 1 (M), LL = 0 (L), S = 0 (L), D = 1 (M)

To calculate *behavior-score* and for the purposes of Experiments I and II, the suggested consequences are all assumed either Low, Medium or High, then mapped to Matrix 1. Whereas for system risk, *system-risk*, an average risk score representing each risk level is assumed as 2, 5.5 and 8.5 for low, medium and high risk levels. For each conscientiousness personality trait level, two types of user accounts are considered, private and public, and both *app-behavior-risk* and *overall-risk* are calculated.

To carry on with experiment I, assumptions I.a, I.b and I.c are made as in Table 7.1.

Assumption	behavioral-related factor		*behavior-score*	*system-risk*	*app-score*	User-centric factor	User behavior	*account-type-score*		*behavior-risk* and *overall-risk*
	auth-score	*connect-score*						Pr	Pb	
I.a	L	L	L	2 (L)	0, 1, 2, 3, 4	Conscientiousness (HC, LC)	Downloading files from suspicious/unknown websites	1	2	As in Figure 7.1
I.b	M	M	M	5.5 (M)						As in Figure 7.2
I.c	H	H	H	8.5 (H)						As in Figure 7.3
II.a	L	M	M	5.5 (M)						As in Figure 7.4
II.b	L	H	H	8.5 (H)						As in Figure 7.5
II.c	M	L	L	2 (L)						As in Figure 7.6
II.d	M	H	H	8.5 (H)						As in Figure 7.7
II.e	H	L	L	2 (L)						As in Figure 7.8
II.f	H	M	M	5.5 (M)						As in Figure 7.9

Table 7.1: Settings of Assumptions I and II Risk Scores/Levels

[1] The terminology "app-" and "sys-" are used interchangeably to differentiate between the *behavior-risk* of an application related behavior and that of a system-related behavior.

After applying the model and calculating risk, different risk scores/levels spanning the entire proposed risk scale are obtained as in Figures 7.1,7.2 and 7.3 where Pr and Pb denote private and public account, HC and LC denote a High and Low level of conscientiousness personality trait respectively. Generally, the higher the risk of behavioral related factors the higher the *app-behavior-risk* and *overall-risk* and vice versa. The resulting risk scores/levels are in line with findings of Chapter 4 as the more conscientiousness the user is, the lower the risk level of his behavior. Actually, even users with the same level of conscientiousness and same score/level of behavioral-related factors do not share the same resulting risk scores/levels. More notably, when comparing between the resulting risk scores/levels of those who scored high in conscientiousness personality trait and those with who scored low, a general trend is observed in all assumptions as the resulting risk scores/levels in private user accounts are lower than those of a public user account. This suggests the granularity and personalized nature of the proposed risk model and the fact that risk is not the same for all users. This is apparent as the *overall-risk* of users, in assumption I.a for instance, with high conscientiousness and a private user account range between 1.5 and 3.8 (low) and from 2.0.(low) to 4.3 (medium) for the same user but with a public account as illustrated in Figure 7.1. Whereas for a user with a lower level of conscientiousness, the *overall-risk* ranged between 1.9 (low) and 4.3 (medium) in a private user account and between 2.3 (low) and 4.7 (medium) for the same user but with a public user account. The same trend was observed in assumptions I.b and I.c as in Figures 7.2 and 7.3.

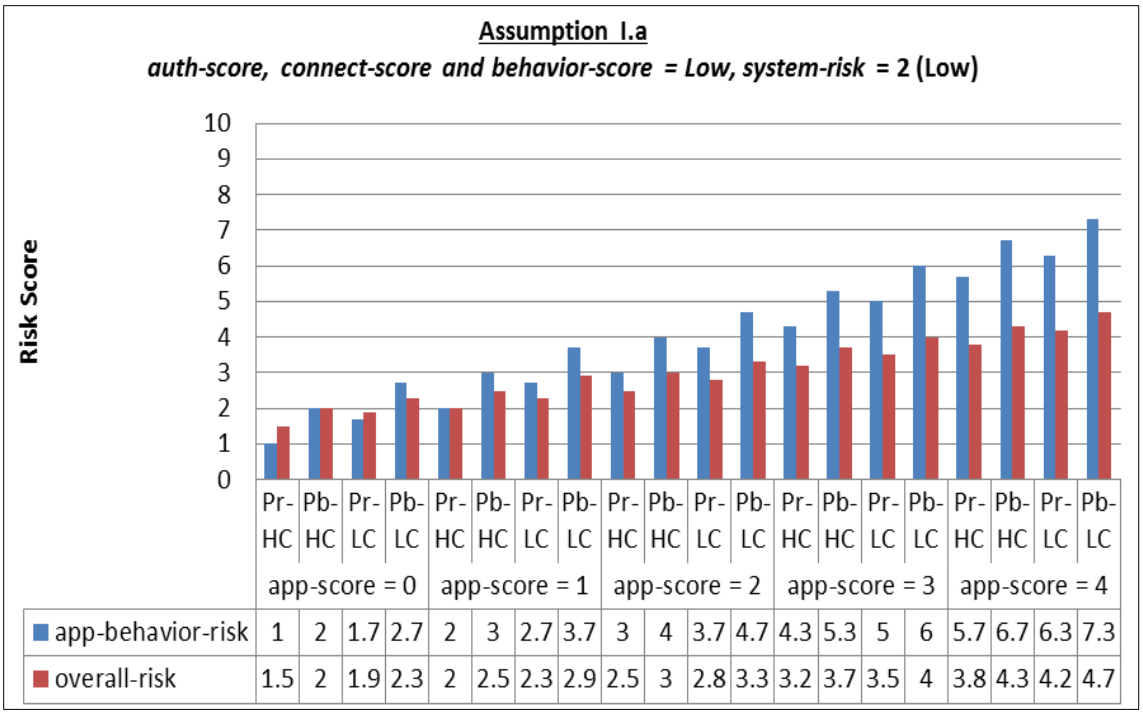

Figure 7.1: Assumption I.a resulting risk scores/levels

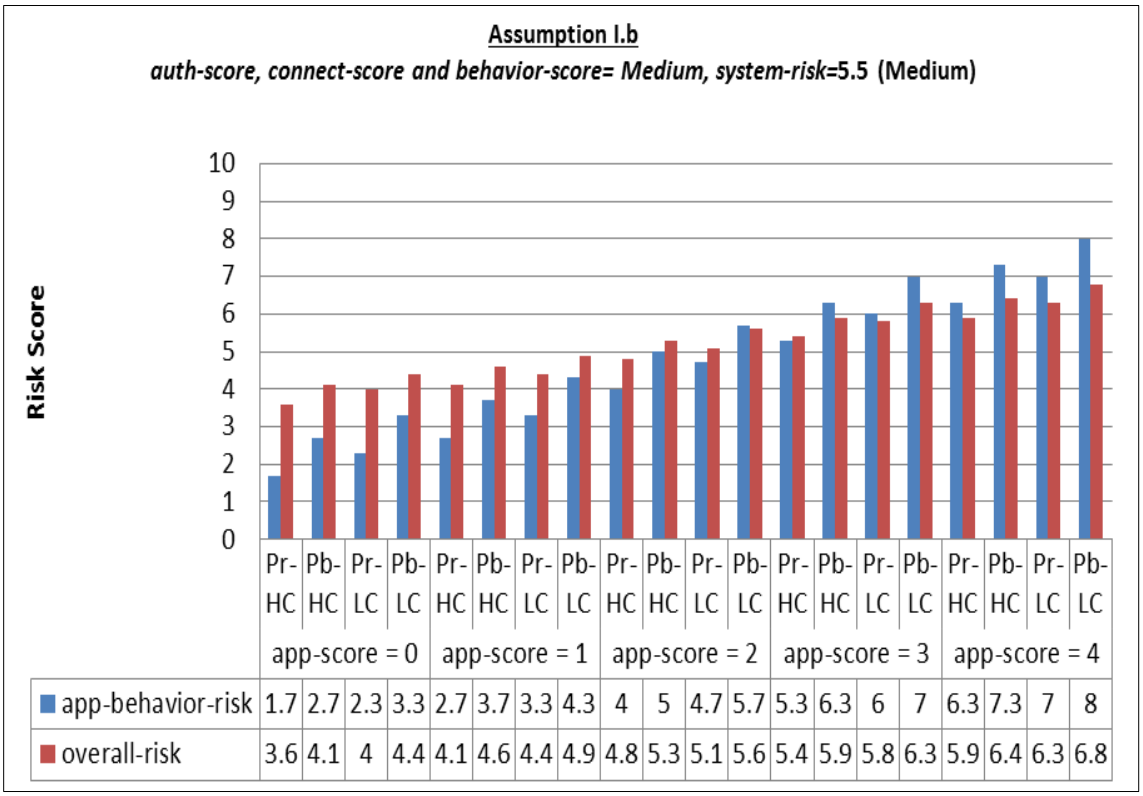

Figure 7.2: Assumption I.b resulting risk scores/levels

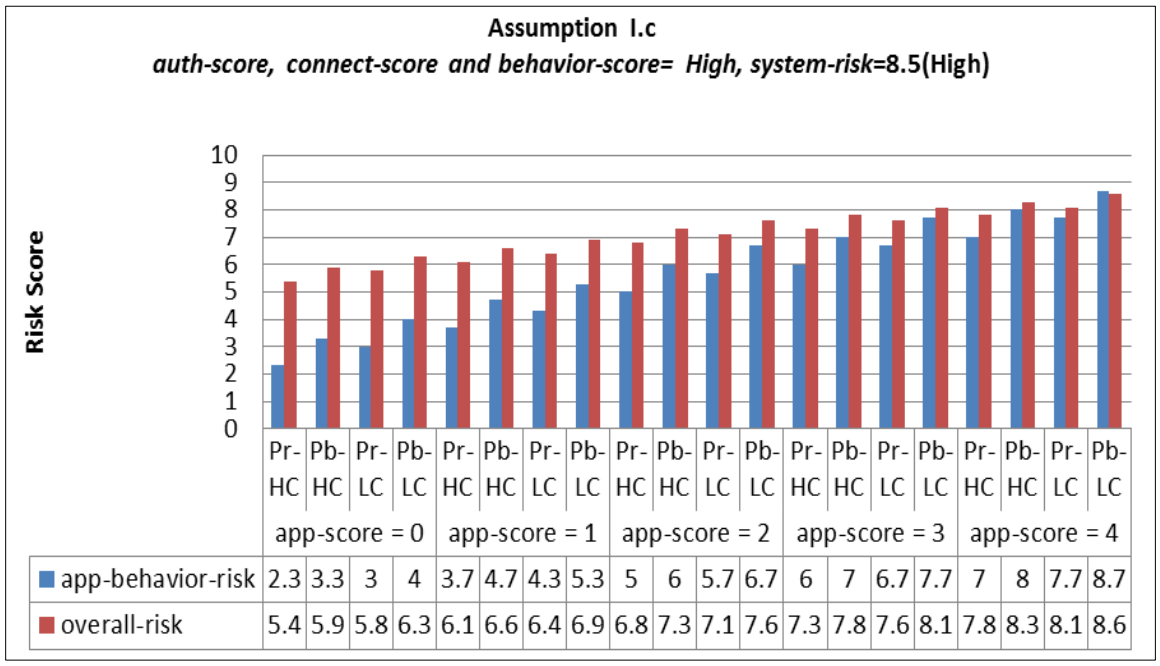

Figure 7.3: Assumption I.c resulting risk scores/levels

From Figures 7.1,7.2 and 7.3, the comparison between *app-behavior-risk* and *overall-risk* offers an indication on the impact of system risk thru the variable *system-risk* on the resulting *overall-risk*. Regardless of the positive relation found between *app-behavior-risk, overall-risk* and behavioral-related factors, an opposing trend was found between *app-behavior-risk* and *overall-risk*. This relation was noted such that whenever *system-risk* is greater than *app-behavior-risk*, then the resulting *overall-risk* is greater than *app-behavior-risk* and vice versa. When *system-risk* is medium with risk score of 5.5 as in assumption I.b Figure 7.2, for example, a high conscientiousness user with a private account and *app-score* = 3, *app-behavior-risk* is 5.3 , i.e less than *system-risk*, the resulting *overall-risk* is 5.4, i.e greater than *app-behavior-risk*. Whereas for the same user but with a public account when *app-behavior-risk* is 6.3, i.e. greater than *system-risk*, the resulting *overall-risk* is less than *app-behavior-risk* with a score of 5.9. This implies that a highly vulnerable system may, arguably, be a bigger threat source to the user than his own behavior.

To further explore the impact of variations in user-centric factors and behavioral-related factors on the resulting risk scores/levels, Experiment II is done. For the same selected user-centric factor of

conscientiousness personality trait and the user behavior of "Downloading files form suspicious/unknown websites" as in Experiment I, the impact of authentication hygiene thru the variable *auth-score* is selected, for instance, as a behavioral-related factor in Experiment II. As such, assumptions II.a, II.b, II.c, II.d, II.e and II.f are made as in Table 7.1 and resulting risk scores are as in Figures 7.4, 7.5, 7.6, 7.7, 7.8 and 7.9 respectively.

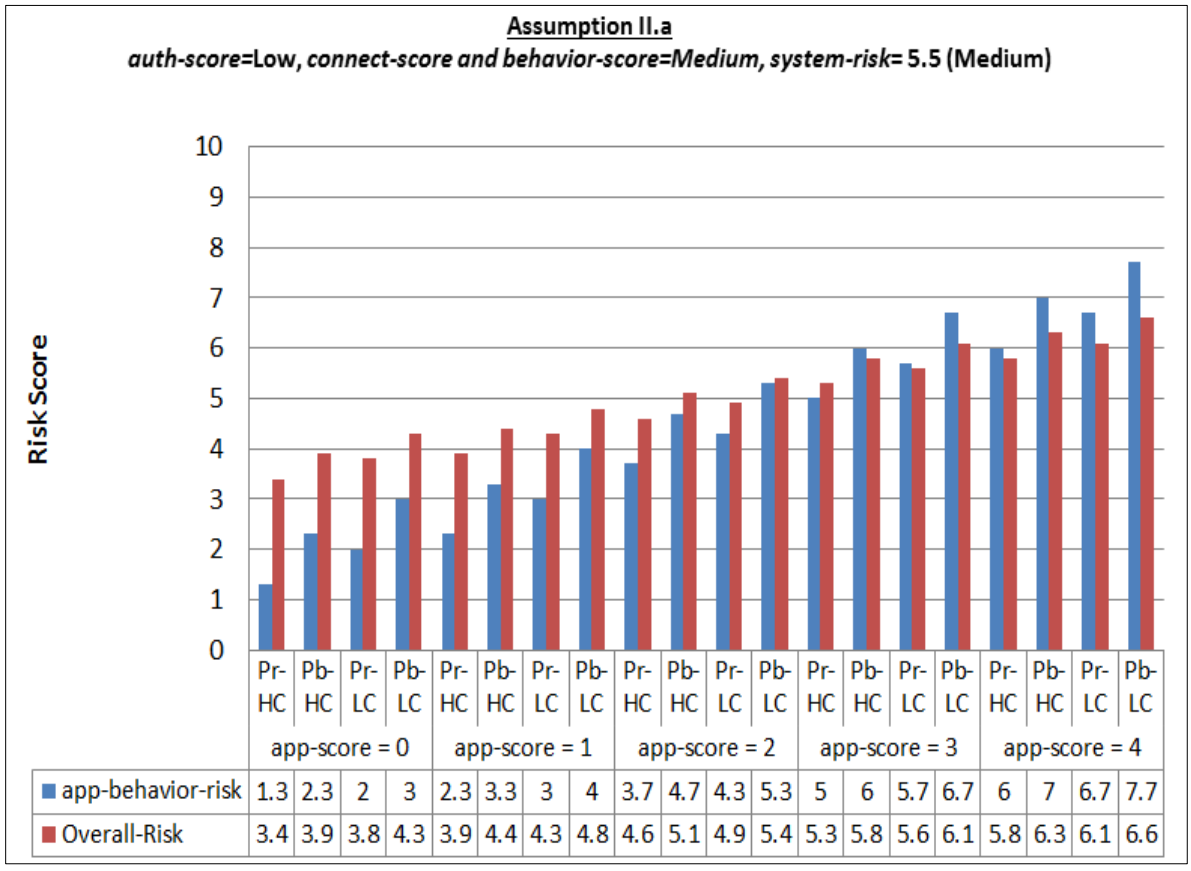

Figure 7.4: Assumption II.a resulting risk scores/levels

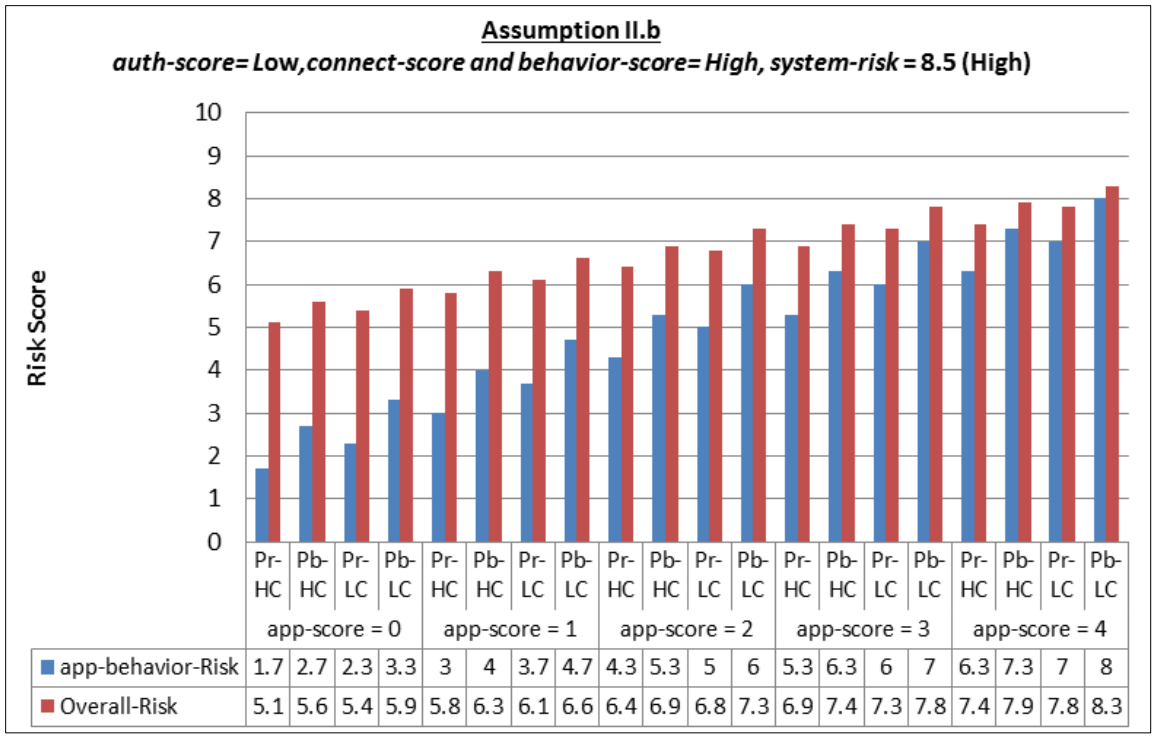

Figure 7.5: Assumption II.b resulting risk scores/levels

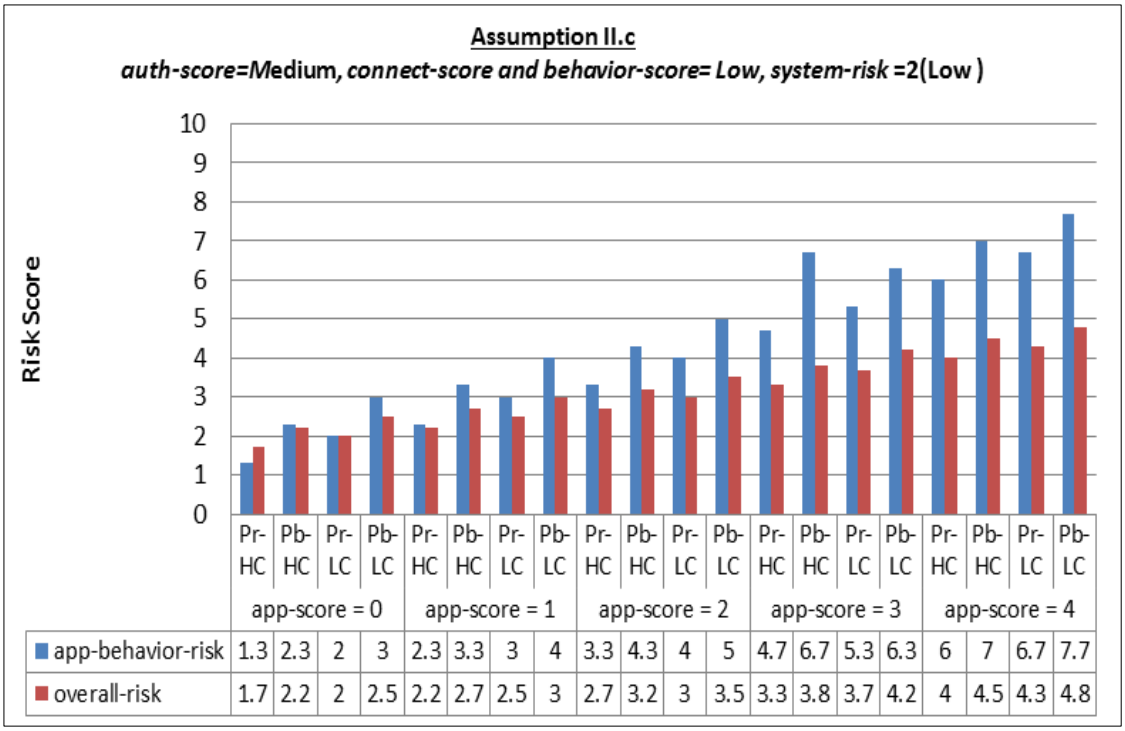

Figure 7.6: Assumption II.c resulting risk scores levels

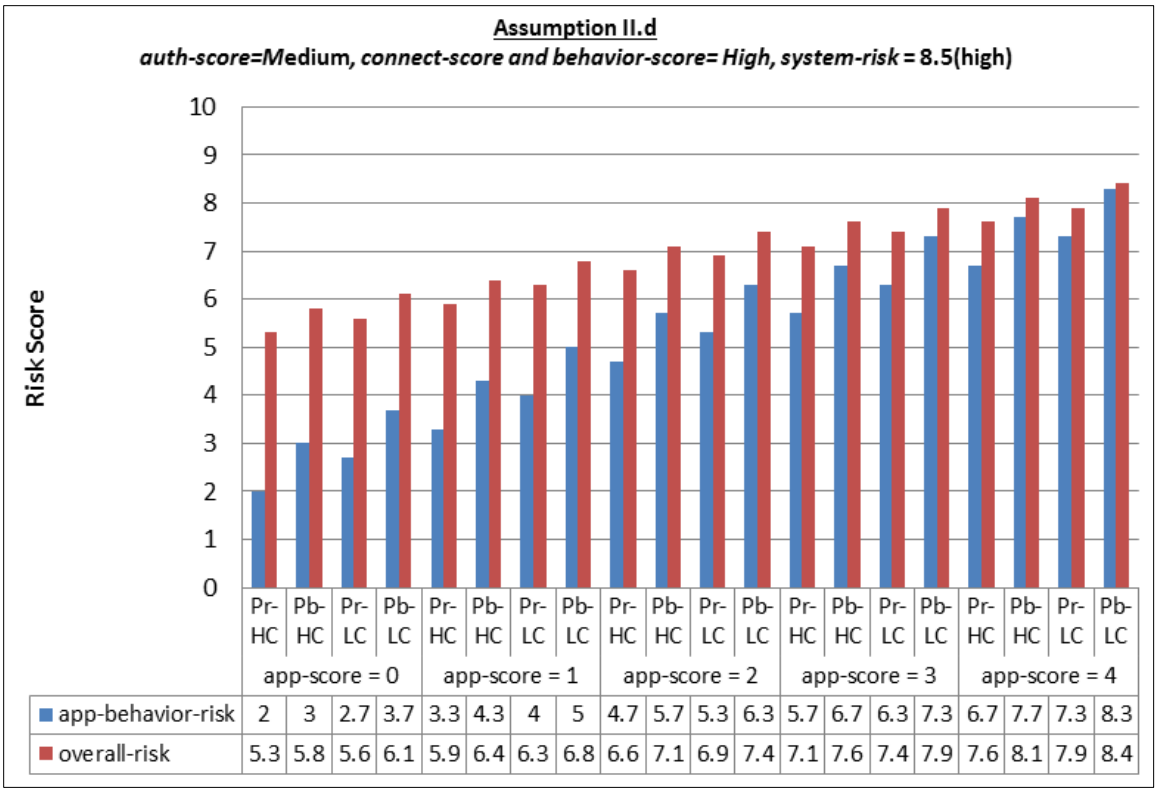

Figure 7.7: Assumption II.d resulting risk scores/levels

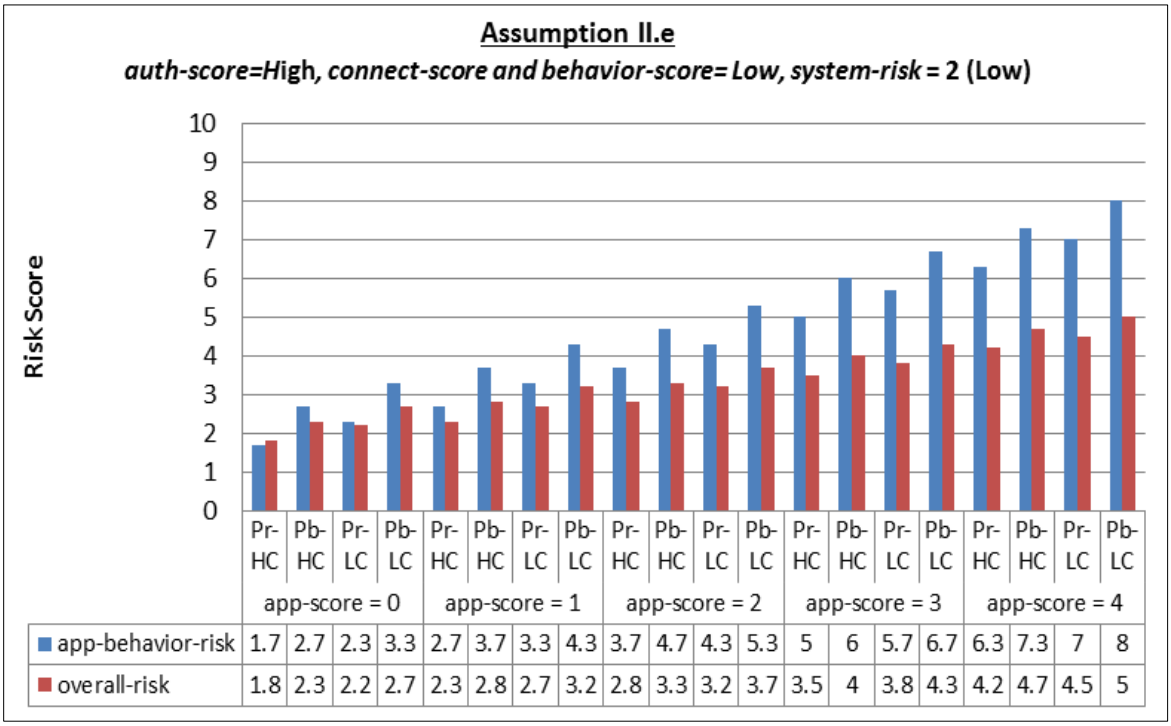

Figure 7.8: Assumption II.e resulting risk scores/levels

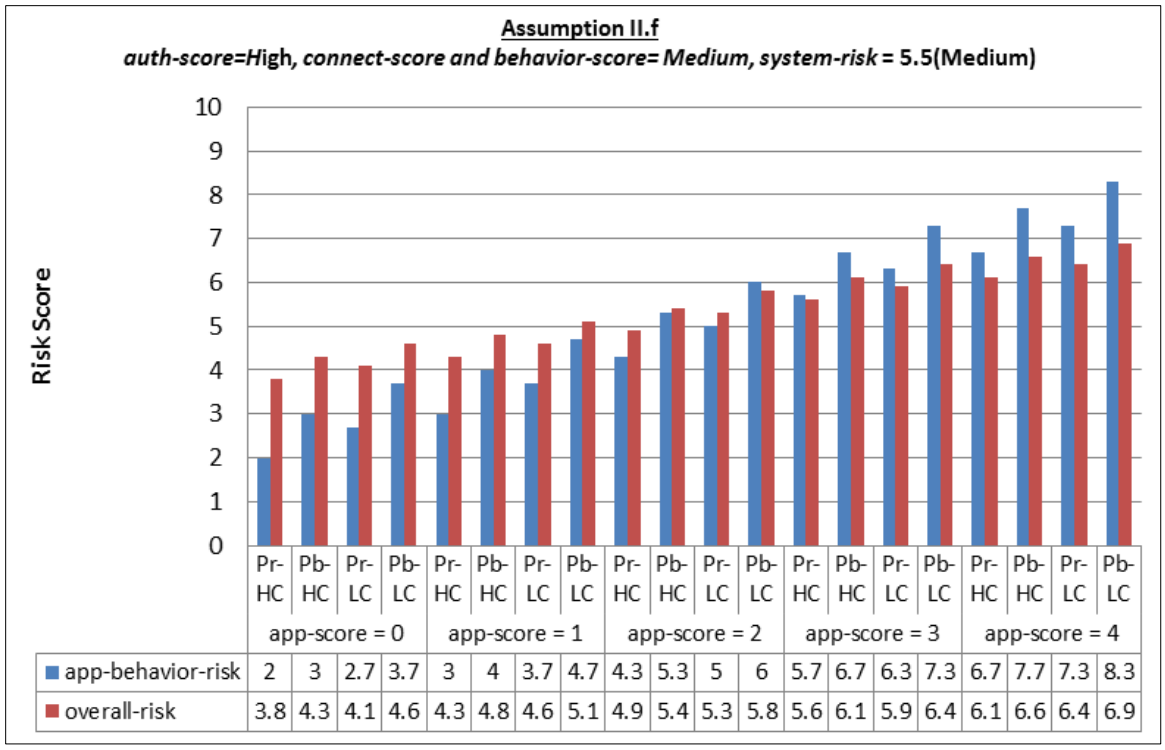

Figure 7.9: Assumption II.f resulting risk scores/levels

Based upon these resulting risk scores/levels, it shows that a similar trend as in Experiment I results is observed in terms of how conscientiousness the user is, type of user account, system-risk score and the resulting risk scores/levels. This suggests that this relation is preserved regardless of the change in behavioral-related factors risk scores/levels. However, this is in contrast to the impact of a change in only one behavioral-related factor on the resulting risk scores/levels as illustrated in Table 7.2. A comparison of the resulting risk scores/levels between assumptions I.b (Figure 7.2) and II.a (Figure 7.4), and between those of assumptions I.c (Figure 7.3) and II.b (Figure 7.5) reveals the relation between *auth-score* and other behavioral-related factors. In the former, when all behavioral-related factors had an equal risk score/ level of medium as in assumption I.b (Figure 7.2) and for the same circumstances but the user is using a password complying to password hygiene rules, i.e. low risk, as in assumption II.a (Figure 7.4), a fixed decrease in both *app-behavior-risk* and *overall-risk* of approximately 0.4 and 0.2 is noted. Whereas in the latter, assumptions I.c (Figure 7.3) and II.b (Figure 7.5), for the same used complying password but with higher risk for other behavioral-related risk factors, a similar relation was found when comparing the

resulting *app-behavior-risk* and *overall-risk* scores. This reveals an increased decrease than of assumptions I.b and II.a as *app-behavior-risk* decreased in approximately 0.7 and the *overall-risk* decreased of 0.3. Regardless of the decreased amount, this comparison highlights the importance and the impact of using a password complying to password hygiene rules. This suggests the impact of authentication as a behavioral-related factor on the resulting risk scores/levels.

However, an opposing relation was found when the risk of authentication is higher, i.e. the user is not using a complying password. This is apparent when comparing between the resulting *app-behavior-risk* and *overall-risk* scores of assumption I.a (Figure 7.1) with those of assumption II.e (Figure 7.8), as a fixed increase of approximately 0.7 and 0.3 between *app-behavior-risk* and *overall-risk* was found. Similarly, when comparing between the resulting *app-behavior-risk* and *overall-risk* scores of assumption I.b (Figure 7.2) with those of assumption II.f (Figure 7.9), a fixed increase of approximately 0.4 and 0.2 was apparent. This suggests the impact of authentication on resulting risk scores/levels such that the higher the risk of authentication the higher the resulting risk scores/levels even if other behavioral-related factors were lower in risk.

When a medium risk password is used, comparing the resulting scores of *app-behavior-risk* and *overall-risk* lead to an interesting observation. The higher the risk of authentication than other behavioral-related factors as in the comparison between assumptions I.a (Figure 7.1) and II.c (Figure 7.6), resulted in an increase in the resulting *app-behavior-risk* and *overall-risk* scores . Conversely, the lower the risk of authentication than other behavioral-related factors as in the comparison between assumptions I.c (Figure 7.3) and II.d (Figure 7.7), resulted in a decrease in the resulting *app-behavior-risk* and *overall-risk* scores.

Given the nature of scoring of both *auth-score* and *connect-score*, i.e scores 0..6, this suggests that these observed relations could be generalized for the connectivity behavioral-related factor.

A similar impact that was found in assumptions of Experiment I of system risk on *overall-risk*, was also found in assumptions of Experiment II. This suggests the contribution of system risk to the user's

risk level even if user's behavior is in low risk, highlighting the importance of keeping operating system and installed applications/software up to date. This highlights the impact behavioral-related factors have on user's risk level and showing that there are factors/risk sources that contribute to user's risk level (compound risk) and should be considered when assessing risk. Even if the user's behavior was considered secure but other behavioral-related factors are not such as the used communication medium or authentication behavior, there is a chance of information disclosure due to an old or reused password for instance.

Comparison between resulting risk scores/level of assumptions:	**Impact on**	
	app-behavior-risk	***overall-risk***
I.b (Figure 7.2)/ II.a (Figure 7.4)	≈ - 0.4	≈ - 0.2
I.c (Figure 7.3)/II.b (Figure 7.5)	≈ - 0.7	≈ - 0.3
I.a (Figure 7.1)/II.e (Figure 7.8)	≈ + 0.7	≈ + 0.3
I.b (Figure 7.2)/ II.f (Figure 7.9)	≈ + 0.4	≈ + 0.2
I.a (Figure 7.1)/ II.c (Figure 7.6)	≈ + 0.3	≈ + 0.2
I.c (Figure 7.3)/ II.d (Figure 7.7)	≈ - 0.3	≈ - 0.2

Table 7.2: Analysis of impact of *auth-score* on resulting risk scores/levels

7.3.2 Scenario-based Simulation

The following scenario is assumed. However, it is worth highlighting that this scenario has no specific basis only that it introduces a number of different risks a typical user might encounter. Hence, assuming the following scenario:

The user is sitting in Starbucks coffee shop and connected to their WiFi. While browsing his email's inbox, he opened an email from an unknown sender asking for his credentials and bank account number to claim a won lottery prize, but ignored it. Then, he opened another email from a friend and downloaded a greeting card that was attached to it. Meanwhile, he was alerted that a new update for his Antivirus application is available, but cancelled it. At that time, a friend came to sit with him where they chatted for an hour. When his friend left, he unlocked his device and started browsing job websites. When a job request was found and wanted to apply for it, he was asked to register with a username and password first. After registration, he was prompted by the browser to remember this password and accepted. Subsequent to signing in, he was redirected to another website unknown to him to download and fill an application

form. Ignoring an alert not to open this document, he opened the document, filled it up and clicked on "SEND". As he was typing the BBC News website's URL, he was alerted that a preinstalled application (Antivirus application) is slowing down his device so he immediately disabled it and continued browsing.

Starbucks's Router is using CISCO AIRONET access point software version 8.1 (112.3). The user is using a Samsung Galaxy Note 3 running Android version 4.4.4, Google Chrome application version 39.0.2171.45 and Email application version 4.2.2.0200. The user is using Symantec Mobile Security as an Antivirus application. Both the email's password and the job website's password comply to all password hygiene attributes except that the former does not contain uppercase letters and the same password is used for his Twitter account while the latter is 5 characters long. The used device pin lock is 1111. The user rated the importance of Twitter application as low (*app-score* = 1), Chrome as medium (*app-score* = 2), Email as High (*app-score* = 3) and Symantec Mobile Security as very high (*app-score* = 4). However, all applications were installed from Google Play which is a legitimate market.

The following types of users are assumed along with their characteristics as in Table 7.3:

User	Personality Traits					Age	Gender	IT Proficiency	Service Usage
	Extra.	Agree.	Con.	Neuro.	Open.				
A	High	Low	Low	High	Low	40 Years	Male	IT Pro.	Low
B	High	High	High	Low	Low	55 Years	Female	Non IT Pro.	Medium
C	Low	Low	High	Low	High	27 Years	Male	IT Pro.	High
D*	High	Low	Low	High	Low	19 Years	Female	Non IT Pro.	High
E**	Low	High	High	Low	High	52 Years	Male	IT Pro.	Low

Table 7.3 : Users' Characteristics

* User with highest risk profile, ** User with lowest risk profile

Given the above scenario, the following is a list of insecure security behaviors along with their behavior type (according to the suggested categorization of user's behaviors as in Figure 6.1) and the user-centric factor that was found to have the most significant correlation with that behavior as in Table 7.4:

B#	Behavior	Behavior Type	Most Significant Characteristic	Correlation
B1	Connecting to a public WiFi	System-Device/ Connectivity	Service Usage	Positive
B2	Same password for multiple Accounts	Application/Authentication	IT proficiency	Negative
B3	Did not delete a suspicious email	Application/ Write - Private data	Age	Negative
B4	Opened an attachment in an email from a friend without checking	Application/ Read -Private data	IT proficiency	Negative
B5	AntiVirus software not updated	System-Device / Settings	IT proficiency	Negative
B6	Cancelled a security related update	System-Device / Responding to alerts	None	None
B7	Did not disable WiFi when not using it	System-Device / Connectivity	Gender	Negative
B8	Device Lock of "1111"	System-Device / Device locking	Con. Personality trait	Negative
B9	Allowed browser to remember his password	Application/ Write - Private data	Service usage	Positive
B10	Opened a document despite security warning	System-Device / Responding to alerts	Age	Negative
B11	Disabled AntiVirus software	Application/ Settings	Con. Personality trait	Negative
B12	Downloaded a file from an unknown website	Application/ Write - Public data	Con. Personality trait	Negative

Table 7.4: A List of Simulation's Users' Insecure Behaviors

Figure 7.10 demonstrates a mapping of the suggested categorization of behaviors to simulation's behavior numbers (B#) as in Table 7.4.

To calculate and estimate risk of the behaviors mentioned in Table 7.4, risk is calculated and assessed on the system level first then on the user level.

I. <u>To calculate risks on the system level, *system risk* :</u>

1. The CVSS scores for Chrome, Email, Symantec Mobile Security applications, Android version 4.4.4 and the router's software are determined.
2. Using the methodology proposed by (Wu and Wang, 2011), the security scores of each of the mentioned applications , *app-risk*, the used Operating System, *os-risk*, and router's software, *nw-risk,* are calculated.

The methodology proposed by (Wu and Wang 2011) is used as follows as of November 2017:

- **For Operating system: Android V. 4.4.4:**
  Total number of vulnerabilities = 122.

  Detailed calculations of the sum of W, P and CVSS of such vulnerabilities are in Appendix C.

Therefore,

OS_Risk = Final score = W1*P1 + W2*P2 + W3*P3 = 2.5 + 1.0 + 3.3 = **6.8 medium risk**

- **For applications:**

  a) Google Chrome for Android v. 39.0.2171.45 : Total number of vulnerabilities = 1

  b) Google Email Application v. 4.2.2.0200 : Total number of vulnerabilities = 1

  c) Symantec Mobile Security v. 1.0 : Total number of vulnerabilities = 1

Detailed calculations of the sum of W, P and CVSS of such vulnerabilities are in Appendix C

Therefore,

App_Risk (Chrome) = Final score = W1*P1 = 5.0*1 = **5.0 medium risk**

App_Risk (Email) = Final score = W1*P1 = 5.0*1 = **5.0 medium risk**

App_Risk (Mobile Security) = Final score = W1*P1 = 4.3*1 = **4.3 medium risk**

- **For Network Router CISCO AIRONET access point software ver. 8.1 (112.3):**
  Total number of vulnerabilities = 3

  Detailed calculations of the sum of W, P and CVSS of such vulnerabilities are in Appendix C.

  Therefore,

NW_Risk = Final score = W1*P1 + W2*P2+ W3*P3= 6.1*0.33 + 7.2*0.33 + 6.1*0.33 = **6.4 medium risk**

Hence, system risk is calculated as follows:

$System\text{-}risk = App\_risk * w_{app} + OS\_risk * w_{os} + NW\_risk * w_{nw} / (w_{app}+w_{os}+w_{nw})$

For the purposes of this research these weights, w_{app}, w_{os} and $w_{nw,}$ are suggested as 0.5, 0.3 and 0.2 respectively. Thus,

system-risk (Chrome) = 5.0*0.5 + 6.8*0.3 + 6.4*0.2 = **5.8 medium risk**

system-risk (Email) = 5.0*0.5 + 6.8*0.3 + 6.4*0.2 = **5.8 medium risk**

system-risk (Mobile Security) = 4.3*0.5 + 6.8*0.3 + 6.40*0.2 = **5.5 medium risk**

II. **To calculate risks on the user level, *behavior- risk* and *overall-risk*:**

For each behavior in Table 7.4, risk of the behavior, *behavior-risk*, is calculated first followed by calculation of aggregated/final risk, *overall-risk*. According to user's rating of used applications, Twitter's *app-score* = 1, Chrome's *app-score* = 2, Email's *app-score* = 3 and Symantec Mobile Security's *app-score* = 4.

B1: Connecting to a public WiFi:

According to the suggested Categorization of behaviors as in Figure 7.10, this is a system/device connectivity behavior. The *behavior-risk* for this particular behavior is calculated as a standalone behavior.

B1.1 The used communication channel is a public WiFi, thus, its assigned risk level is high.

behavior-score= (7+10)/2 = 8.5

B1.2 Based on findings of Chapter 4 and the proposed significance correlation risk factor methodology, the user-centric factor of service usage level has the most significant positive correlation with this behavior. Hence, *behavior-risk* is recalculated independently for each user.

IF service usage level = High THEN (Users C and D)

Risk of behavior is increased such that

behavior-score = *behavior-score* + 1 = 9.5 = *behavior-risk*

and *overall-risk* = *behavior-risk* = 9.5 high risk

IF service usage level = low THEN (Users A and E)

Risk of behavior is decreased such that

behavior-score = *behavior-score* - 1 = 7.5 = *behavior-risk*

and *overall-risk* = *behavior-risk* = 7.5 high risk

IF service usage level = medium THEN (User B)

Risk of behavior is neither decreased nor increased such that

behavior-score = 8.5 = *behavior-risk*

and *overall-risk* = *behavior-risk* = 8.5 high risk

B2: Same password for multiple Accounts:

According to the suggested Taxonomy of behaviors as in Figure 7.10, this is an application-related authentication behavior. The *behavior-risk* for this particular behavior is calculated as a standalone behavior. The user rated the importance of Twitter application as low, i.e. *app-score* = 1, and Email application as high, i.e. *app-score* = 3. According to the proposed model, the highest *app-score* will be considered when calculating *behavior-risk*. This behavior is considered with the reuse attribute of password hygiene attributes.

B2.1 The risk of this behavior is high. The *behavior-score* depends on *app-score*. Thus , by mapping the *app-score* and high risk in Matrix 2

behavior-score = 5

		Reuse		
		Low	Medium	High
app-score	0	0	1	2
	1	1	2	3
	2	2	3	4
	3	3	4	**5***
	4	4	5	6

B2.2 Based on findings of Chapter 4, the user-centric factor of IT proficiency has the most significant negative correlation with this behavior. Hence, according to the proposed model for calculating the significance correlation risk factor, *behavior-score* is recalculated and normalized independently for each user as follows:

IF IT proficiency = non-IT professional (low) THEN (Users B and D)

An opposite mapping will occur by mapping the user's IT proficiency group to high. In Matrix 3, the pre-calculated *behavior-score* = 5 is mapped to high risk and *app-score* =3. Therefore, the resulting *behavior-score* = 7

IT proficiency group		Low			High		
behavior-score		L	M	H	L	M	H
App-score	0	0	1	2	2	3	4
	1	1	2	3	3	4	5
	2	2	3	4	4	5	6
	3	3	4	5	5	6	**7***
	4	4	5	6	6	7	8

behavior-risk= *behavior-score* * 1.25 = 7 * 1.25 = 8.8

The final risk score/level, *Overall-risk* = (*behavior-risk** W_{br})+ (*system-risk* *W_{sr})

where $W_{br=} W_{sr =}$ 0.5. Thus,

Overall-risk = (8.8 * 0.5) + (5.8 * 0.5) = 7.3 High Risk

IF IT proficiency = IT professional (high) THEN (Users A, C and E)

An opposite mapping will occur by mapping the user's IT proficiency group to low. In Matrix 3, the pre-calculated *behavior-score* = 5 is mapped to high risk and *app-score* = 3. Therefore, the resulting *behavior-score* = 5

IT proficiency group		Low			High		
behavior-score		L	M	H	L	M	H
App-score	0	0	1	2	2	3	4
	1	1	2	3	3	4	5
	2	2	3	4	4	5	6
	3	3	4	**5***	5	6	7
	4	4	5	6	6	7	8

behavior-risk= *behavior-score* * 1.25 = 5* 1.25 = 6.3

The final risk score/level, *Overall-risk-score* = (*behavior-risk** W_{br})+ (*system-risk* *W_{sr})
where $W_{br=} W_{sr =}$ 0.5. Thus,

Overall-risk-score = (6.3 * 0.5) + (5.8 * 0.5) = **6.1 medium risk**

B3: Did not delete a suspicious email:

According to the suggested categorization of behaviors as in Figure 7.10, this is an application-related/ wirte private data behavior. As of the proposed model, risk is calculated as:

behavior-risk=AVG(*behavior-score*, *auth-score*, *connect-score*)+*account-type-score*

Therefore,

B3.1 According to user's importance rating, Email application *app-score* = 3.

B3.2 The account type for this application is considered as private, thus *account-type-score*=1.

B3.3 The used communication channel is a public WiFi, thus, its assigned risk level is high. By mapping both *app-score* and connectivity risk level in Matrix 4, the risk of this communication channel, *connect-score* = 5

		Connectivity		
		Low (such as wired private network and 3G/4G)	Medium (such as Bluetooth, NFC and Private WiFi)	High (such as Public WiFi)
app-score	0	0	1	2
	1	1	2	3
	2	2	3	4
	3	3	4	**5***
	4	4	5	6

B3.4 The used password is assessed for its hygiene using Matrix 1. The password complies to all password hygiene attributes (i.e. low risk) except for its reuse and uppercase attributes. Password does not have uppercase letters and is reused (shared) in Twitter account, thus, high risk for these particular attributes. By mapping these risk levels and the *app-score* in Matrix 1,

auth-score = Max (length, reuse, old, uppercase, lowercase, characters, numbers)

= Max (3, 5, 3, 5, 3, 3, 3) = 5

		Password Attributes																				
		Length			Reuse			Old			Uppercase			Lowercase			Characters			Numbers		
		L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
app-score	0	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
	1	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
	2	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4
	3	**3***	4	5	3	4	**5***	**3***	4	5	3	4	**5***	**3***	4	5	**3***	4	5	**3***	4	5
	4	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6

B3.5 This particular behavior is a write-private data and its suggested consequences are

E=1 (M), F=2 (H), P=2 (H), DC=2 (H), LL=1 (M), S=0 (L), D=0 (L)

By mapping these consequences and the *app-score* in Matrix 2,

behavior-score = Max (E, F, P, DC, LL, S, D)

= Max (4,5,5,5,4,3,3) = 5

		Consequences																				
		E			F			P			DC			LL			S			D		
		L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
app-score	0	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
	1	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
	2	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4
	3	3	**4***	5	3	4	**5***	3	4	**5***	3	4	**5***	3	**4***	5	**3***	4	5	**3***	4	5
	4	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6

B3.6 Based on findings of Chapter 4, the user-centric factor of age has the most significant negative correlation with this behavior. Hence, according to the proposed model for calculating the significance correlation risk factor, *behavior-score* is recalculated independently for each user as follows:

IF age = 18-30 years (low) THEN (Users C and D)

An opposite mapping will occur by mapping the user's age group to high. In Matrix 3, the pre-calculated *behavior-score* = 5 is mapped to high risk and *app-score* =3. Therefore, the resulting *behavior-score* = 7

Age group		Low			Medium			High		
behavior-score		L	M	H	L	M	H	L	M	H
App-score	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	**7***
	4	4	5	6	5	6	7	6	7	8

behavior-risk=AVG(*behavior-score*, *auth-score*, *connect-score*)+*account-type-score*

= AVG (7, 5, 5) +1 = 6.7

The final risk score/level, *Overall-risk* = (*behavior-risk** W_{br})+ (*system-risk* *W_{sr})

where $W_{br=}$ W_{sr} = 0.5. Thus,

Overall-risk = (6.7 * 0.5) + (5.8 * 0.5) = **6.3 medium risk**

IF age = 51+ years (high) THEN (users B and E)

An opposite mapping will occur by mapping the user's age group to low. In Matrix 3, the pre-calculated *behavior-score* = 5 is mapped to high risk and *app-score* =3. Therefore, the resulting *behavior-score* = 5

Age group		Low			Medium			High		
behavior-score		L	M	H	L	M	H	L	M	H
App-score	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	**5***	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

behavior-risk=AVG(*behavior-score*, *auth-score*, *connect-score*)+*account-type-score*
= AVG (5, 5, 5) +1 = 6

The final risk score/level, *Overall-risk* = (behavior-risk* W_{br})+ (system-risk *W_{sr})

where $W_{br=}$ $W_{sr=}$ 0.5. Thus,

Overall-risk = (6 * 0.5) + (5.8 * 0.5) = **5.9 medium risk**

IF age = 31-50 years (Medium) THEN {User A}

Age group is mapped to medium. In Matrix 3, the pre-calculated *behavior-score* = 5 is mapped to high risk and *app-score* =3. Therefore, the resulting *behavior-score* = 6

Age group		Low			Medium			High		
behavior-score		L	M	H	L	M	H	L	M	H
App-score	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	**6***	5	6	7
	4	4	5	6	5	6	7	6	7	8

behavior-risk=AVG(*behavior-score*, a*uth-score*, *connect-score*)+*account-type-score*
= AVG (6, 5, 5) +1 = 6.3

The final risk score/level, *Overall-risk* = (*behavior-risk** W_{br})+ (*system-risk* *W_{sr})

where $W_{br=}$ $W_{sr=}$ 0.5. Thus,

Overall-risk = (6.3 * 0.5) + (5.8 * 0.5) = **6.1 medium risk**

This particular behavior is considered to be not good practice. By interpreting the resulting *overall-risk* score, risk decreases with age. Hence, the older the user the lower the risk. This is in-line with the findings of Chapter 4.

B4: Opened an attachment in an email from a friend without checking

According to the suggested categorization of behaviors as in Figure 7.10, this is an application-related/ read private data behavior. As of the proposed model, risk is calculated as:

behavior-risk=AVG(*behavior-score*, *auth-score*, *connect-score*)+*account-type-score*

Therefore, B4.1, B4.2, B4.3 and B4.4 are similar to B3.1, B3.2, B3.3 and B3.4 respectively.

B4.5 This particular behavior is a read-private data and its suggested consequences are

E=2 (H), F=0 (L), P=2 (H), DC=2 (H), LL=0 (L), S=0 (L), D=1 (M)

By mapping these consequences and the *app-score* in Matrix 2,

behavior-score = Max (E, F, P, DC, LL, S, D)

= Max (5,3,5,5,3,3,4) = 5

		Consequences																				
		E			F			P			DC			LL			S			D		
		L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
app-score	0	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
	1	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
	2	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4
	3	3	4	**5***	**3***	4	5	3	4	**5***	3	4	**5***	**3***	4	5	**3***	4	5	3	**4***	5
	4	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6

B4.6 Based on findings of Chapter 4, the user-centric factor of IT proficiency has the most significant negative correlation with this behavior. Hence, according to the proposed model for calculating the significance correlation risk factor, *behavior-score* is recalculated independently for each user as follows:

IF IT proficiency = non-IT professional (low) THEN (Users B and D)

An opposite mapping will occur by mapping the user's IT-proficiency group to high. In Matrix 3, the pre-calculated *behavior-score* = 5 is mapped to high risk and *app-score* =3. Therefore, the resulting *behavior-score* = 7

IT proficiency group		Low			High		
behavior-score		L	M	H	L	M	H
App-score	0	0	1	2	2	3	4
	1	1	2	3	3	4	5
	2	2	3	4	4	5	6
	3	3	4	5	5	6	**7***
	4	4	5	6	6	7	8

behavior-risk=AVG(*behavior-score*, *auth-score*, *connect-score*)+*account-type-score*
= AVG (7, 5, 5) +1 = 6.7

The final risk score/level, *Overall-risk* = (*behavior-risk** W_{br})+ (*system-risk* *W_{sr})

where $W_{br=}$ W_{sr} = 0.5. Thus,

Overall-risk = (6.7 * 0.5) + (5.8 * 0.5) = **6.3 medium risk**

IF IT proficiency = IT-Professional (high) THEN (Users A, C and E)

An opposite mapping will occur by mapping the user's IT-proficiency group to low. In Matrix 3, the pre-calculated *behavior-score* = 5 is mapped to high risk and *app-score* =3. Therefore, the resulting *behavior-score* = 5

IT proficiency group		Low			High		
behavior-score		L	M	H	L	M	H
App-score	0	0	1	2	2	3	4
	1	1	2	3	3	4	5
	2	2	3	4	4	5	6
	3	3	4	**5***	5	6	7
	4	4	5	6	6	7	8

behavior-risk=AVG(*behavior-score*, *auth-score*, *connect-score*)+*account-type-score*
= AVG (5, 5, 5) +1 = 6

The final risk score/level, *Overall-risk* = (*behavior-risk** W_{br})+ (*system-risk* *W_{sr})

where $W_{br=} W_{sr =}$ 0.5. Thus,

Overall-risk = (6 * 0.5) + (5.8 * 0.5) = **5.9 medium risk**

This particular behavior is considered to be not good practice. By interpreting the resulting *overall-risk* score, due to users A, C and E IT proficiency they were in lower risk than others. This is in-line with the findings of Chapter 4.

B5: AntiVirus software not updated:

According to the suggested categorization of behaviors as in Figure 7.10, this is a system/device related settings behavior. The *behavior-risk* for this particular behavior is calculated as a standalone behavior.

B5.1 The installed Anti-Virus application (Symantec Mobile Security) is not updated, thus, its assigned risk level is high.

behavior-score = (7+10)/2 = 8.5 high risk

B5.2 Based on findings of Chapter 4 and the proposed significance correlation risk factor, the user-centric factor of IT proficiency has the most significant negative correlation with this behavior. Hence, *behavior-score* is recalculated independently for each user.

IF IT proficiency = IT professional (High) THEN (Users A, C and E)
Risk of behavior is decreased such that
behavior-score = *behavior-score* - 1 = 7.5 = *behavior-risk*
and *overall-risk* = *behavior-risk* = 7.5 high risk

IF IT proficiency = Non-IT professional (low) THEN (Users B and D)
Risk of behavior is increased such that
behavior-score = *behavior-score* + 1 = 9.5 = *behavior-risk*
and *overall-risk* = *behavior-risk* = 9.5 high risk

B6: Cancelled a security related update:

According to the suggested categorization of behaviors as in Figure 7.10, this is a system/device-related responding to alerts behavior. The *behavior-risk* for this particular behavior is calculated as a standalone behavior.

B6.1 The risk of this behavior is high, thus

behavior-score = (7+10)/2 = 8.5 high risk

B6.2 Based on findings of Chapter 4, no user-centric factor was found to have a significant correlation with this behavior. This implies that no individualized risk calculation is done and all users will share the same resulting risk scores\levels. Hence,

behavior-score = *behavior-risk* = *overall-risk* = 8.5 high risk

B6.3 Since this update was concerned with the installed Anti-Virus Application, the *overall-risk* will be displayed to the user along with the calculated vulnerability score (Wu, Wang, 2011) of Symantec Mobile Security which is **4.3 medium risk**.

B7: Did not disable WiFi when not using it:

According to the suggested categorization of behaviors as in Figure 7.10, this is a system/device-related connectivity behavior. The *behavior-risk* for this particular behavior is calculated as a standalone behavior.

B7.1 According to Matrix 4, connecting to a public WiFi is high risk regardless of *app-score*. Thus,

behavior-score = 8.5

B7.2 Based on findings of Chapter 4 and the proposed significance correlation risk factor, the user-centric factor of gender has the most significant negative correlation with this behavior. Hence, *behavior-score* is recalculated independently for each user.

IF gender = male (High) THEN (Users A, C and E)

Risk of behavior is decreased such that

behavior-score = *behavior-score* - 1 = 7.5 = *behavior-risk*

and *overall-risk* = *behavior-risk* = 7.5 high risk

IF gender = female (low) THEN (Users B and D)

Risk of behavior is increased such that

behavior-score = *behavior-score* + 1 = 9.5 = *behavior-risk*

and *overall-risk* = *behavior-risk* = 9.5 high risk

B8: Device Lock of "1111":

According to the suggested categorization of behaviors as in Figure 7.10, this is a system/device-related device locking behavior. The *behavior-risk* for this particular behavior is calculated as a standalone behavior.

B8.1 The used PIN is assessed for its hygiene using Matrix 5. The suggested PIN hygiene attributes are reuse, old, same number and predictable numbers. The PIN complies to all PIN hygiene attributes (i.e. low risk = 0) except for its same number attribute, thus, high risk for this particular attribute. By mapping these risk levels,

behavior-score = MAX (reuse, old, same number, predictable numbers)

= MAX (0, 0, 7, 0) = 7

	PIN Attributes											
	Reuse			Old			Same Number			Predictable numbers		
	L	M	H	L	M	H	L	M	H	L	M	H
Consequences	**0***	4	7	**0***	4	7	0	4	7*	**0***	4	7

B8.2 Based on findings of Chapter 4 and the proposed significance correlation risk factor, the user-centric factor of conscientiousness personality trait has the most significant negative correlation with this behavior. Hence, *behavior-score* is recalculated independently for each user.

IF conscientiousness = High THEN (Users B, C and E)

Risk of behavior is decreased such that

behavior-score = *behavior-score* - 1 = 7 – 1 = 6 = *behavior-risk*

and *overall-risk* = *behavior-risk* = **6 medium risk**

IF conscientiousness = low THEN (Users A and D)

Risk of behavior is increased such that

behavior-score = *behavior-score* + 1 = 7 + 1 = 8 = *behavior-risk*

and *overall-risk* = *behavior-risk* = 8 high risk

B9: Allowed browser to remember his password:

According to the suggested categorization of behaviors as in Figure 7.10, this is an application-related/ write private data behavior. As of the proposed model, risk is calculated as:

behavior-risk=AVG(*behavior-score*, *auth-score*, *connect-score*)+*account-type-score*

Therefore,

B9.1 According to user's importance rating, Chrome application *app-score* = 2.

B9.2 The account type for this application is considered as private, thus *account-type-score*=1.

B9.3 The used communication channel is a public WiFi, thus, its assigned risk level is high. By mapping both *app-score* and connectivity risk level in Matrix 4, the risk of this communication channel, *connect-score* = 4

		Connectivity		
		Low (such as wired private network and 3G/4G)	Medium (such as Bluetooth, NFC and Private WiFi)	High (such as Public WiFi)
app-score	0	0	1	2
	1	1	2	3
	2	2	3	**4***
	3	3	4	5
	4	4	5	6

B9.4 The used password is assessed for its hygiene using Matrix 1. The password complies to all password hygiene attributes (i.e. low risk) except for its length. Password is five characters long, thus, high risk for this particular attribute. By mapping these risk levels and the *app-score* in Matrix 1,

auth-score = MAX (length, reuse, old, uppercase, lowercase, characters, numbers)

= MAX (4, 2, 2, 2, 2, 2, 2) = 4

		Password Attributes																				
		Length			Reuse			Old			Uppercase			Lowercase			Characters			Numbers		
		L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
app-score	0	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
	1	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
	2	2	3	**4***	**2***	3	4	**2***	3	4	**2***	3	4	**2***	3	4	**2***	3	4	**2***	3	4
	3	3	4	5	3	4	5	3	4	5	3	4	5	3	4	5	3	4	5	3	4	5
	4	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6

B9.5 This particular behavior is an application-related write-private data and its suggested consequences are

E=1 (M), F=2 (H), P=2 (H), DC=2 (H), LL=1 (M), S=0 (L), D=0 (L)

By mapping these consequences and the *app-score* in Matrix 2,

behavior-score = MAX (E, F, P, DC, LL, S, D)

= MAX (3, 4, 4, 4, 3, 2, 2) = 4

		Consequences																				
		E			F			P			DC			LL			S			D		
		L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
app-score	0	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
	1	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
	2	2	**3***	4	2	3	**4***	2	3	**4***	2	3	**4***	2	**3***	4	**2***	3	4	**2***	3	4
	3	3	4	5	3	4	5	3	4	5	3	4	5	3	4	5	3	4	5	3	4	5
	4	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6

B9.6 Based on findings of Chapter 4, the user-centric factor of service usage level has the most significant positive correlation with this behavior. Hence, according to the proposed model for calculating the significance correlation risk factor, *behavior-score* is recalculated independently for each user as follows:

IF service usage level = low THEN (Users A and E)

The user's service usage level is mapped to low. In Matrix 3, the pre-calculated *behavior-score* = 4 is mapped to high risk and *app-score* =2. Therefore, the resulting *behavior-score* = 4

Service usage level		Low			Medium			High		
behavior-score		L	M	H	L	M	H	L	M	H
App-score	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	**4***	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

behavior-risk=AVG(*behavior-score*, *auth-score*, *connect-score*)+*account-type-score*

= AVG (4, 4, 4) +1 = 5

The final risk score/level, *Overall-risk* = (behavior-risk* W_{br})+ (system-risk *W_{sr})

where $W_{br=}$ $W_{sr=}$ 0.5. Thus,

Overall-risk = (5 * 0.5) + (5.8 * 0.5) = **5.4 medium risk**

IF service usage level = high THEN (Users C and D)

The user's service usage level is mapped to high. In Matrix 3, the pre-calculated *behavior-score* = 4 is mapped to high risk and *app-score* =2. Therefore, the resulting *behavior-score* = 6

Service usage level		Low			Medium			High		
behavior-score		L	M	H	L	M	H	L	M	H
App-score	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	**6***
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

behavior-risk=AVG(*behavior-score*, *auth-score*, *connect-score*)+*account-type-score*

= AVG (6, 4, 4) +1 = 5.7

The final risk score/level, *Overall-risk* = (behavior-risk* W_{br})+ (system-risk *W_{sr})

where $W_{br=}$ $W_{sr=}$ 0.5. Thus,

Overall-risk = (5.7 * 0.5) + (5.8 * 0.5) = **5.8 medium risk**

IF service usage level = Medium THEN (User B)

Service usage level is mapped to medium. In Matrix 3, the pre-calculated *behavior-score* = 4 is mapped to high risk and *app-score* =2. Therefore, the resulting *behavior-score* = 5

Service usage level		Low			Medium			High		
behavior-score		L	M	H	L	M	H	L	M	H
App-score	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	**5***	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

behavior-risk=AVG(*behavior-score*, *auth-score*, *connect-score*)+*account-type-score*

= AVG (5, 4, 4) +1 = 5.3

The final risk score/level, *Overall-risk* = (behavior-risk* W_{br})+ (system-risk *W_{sr})

where $W_{br=}$ W_{sr} = 0.5. Thus,

Overall-risk = (5.3 * 0.5) + (5.8 * 0.5) = **5.6 medium risk**

This particular behavior is considered to be not good practice. By interpreting the resulting *overall-risk score*, risk decreases with service usage level. Hence, the lower the service usage the lower the risk. This is in-line with the findings of Chapter 4.

B10: Opened a document despite security warning:

According to the suggested categorization of behaviors as in Figure 7.10, this is a system/device-related responding to alerts behavior. The *behavior-risk* for this particular behavior is calculated as a standalone behavior.

B10.1 The risk of this behavior is high, thus

behavior-score = 8.5

B10.2 Based on findings of Chapter 4 and the proposed significance correlation risk factor methodology, the user-centric factor of age has the most significant negative correlation with this behavior. Hence, *behavior-risk* is recalculated independently for each user.

IF age = 18-30 years (low) THEN (Users C and D)
Risk of behavior is increased such that
behavior-score = *behavior-score* + 1 = 9.5 = *behavior-risk*
and *overall-risk* = *behavior-risk* = 9.5 high risk

IF age = 51+ years (High) THEN (Users B and E)
Risk of behavior is decreased such that
behavior-score = *behavior-score* - 1 = 7.5 = *behavior-risk*
and *overall-risk* = *behavior-risk* = 7.5 high risk

IF age = 31-50 years (medium) THEN (User A)
Risk of behavior is neither decreased nor increased such that
behavior-score = 8.5 = *behavior-risk*
and *overall-risk* = *behavior-risk* = 8.5 high risk

B11: Disabled AntiVirus software:

According to the suggested categorization of behaviors as in Figure 7.10, this is an application-related settings behavior. The *behavior-risk* for this particular behavior is calculated as a standalone behavior. The user rated the importance of this application as very high, hence, *app-score* = 4.

B11.1 The risk of this behavior is high. The *behavior-score* depends on *app-score* in Matrix 1. Thus, *behavior-score* = 6

		Consequence		
		Low	Medium	High
app-score	0	0	1	2
	1	1	2	3
	2	2	3	4
	3	3	4	5
	4	4	5	**6***

B11.2 Based on findings of Chapter 4, the user-centric factor of conscientiousness personality trait has the most significant negative correlation with this behavior. Hence, according to the proposed model for

calculating the significance correlation risk factor, *behavior-score* is recalculated and normalized independently for each user as follows:

IF conscientiousness = low THEN (Users A and D)

An opposite mapping will occur by mapping the user's conscientiousness group to high. In Matrix 3, the pre-calculated *behavior-score* = 6 is mapped to high risk and *app-score* =4. Therefore, the resulting *behavior-score* = 8

Conscientiousness group		Low			High		
behavior-score		L	M	H	L	M	H
App-score	0	0	1	2	2	3	4
	1	1	2	3	3	4	5
	2	2	3	4	4	5	6
	3	3	4	5	5	6	7
	4	4	5	6	6	7	**8***

behavior-risk= behavior-score * 1.25 = 10

The final risk score/level, *Overall-risk* = (behavior-risk* W_{br})+ (system-risk *W_{sr})

where $W_{br=}$ W_{sr} = 0.5. Thus,

Overall-risk = (10 * 0.5) + (5.5 * 0.5) = 7.8 high risk

IF conscientiousness = high THEN (Users B, C and E)

An opposite mapping will occur by mapping the user's conscientiousness group to low. In Matrix 3, the pre-calculated *behavior-score* = 6 is mapped to high risk and *app-score* =4. Therefore, the resulting *behavior-score* = 6

Conscientiousness group		Low			High		
behavior-score		L	M	H	L	M	H
App-score	0	0	1	2	2	3	4
	1	1	2	3	3	4	5
	2	2	3	4	4	5	6
	3	3	4	5	5	6	7
	4	4	5	**6***	6	7	8

behavior-risk= behavior-score * 1.25 = 7.5

The final risk score/level, *Overall-risk* = (behavior-risk* W_{br})+ (system-risk *W_{sr})

where $W_{br=} W_{sr=}$ 0.5. Thus,

Overall-risk = (7.5 * 0.5) + (5.5 * 0.5) = **6.5 medium risk**

B12: Downloaded a file from an unknown website:

According to the suggested categorization of behaviors as in Figure 7.10, this is an application-related/ write public data behavior. As of the proposed model, risk is calculated as:

behavior-risk=AVG(*behavior-score*, *auth-score*, *connect-score)+account-type-score*

Therefore,

B12.1, B12.2, B12.3 and B12.4 are similar to B9.1, B9.2, B9.3 and B9.4 respectively.

B12.5 This particular behavior is an application-related write-public data and its suggested consequences are

E=1 (M), F=0 (L), P=1 (M), DC=1 (M), LL=0 (L), S=0 (L), D=1 (M)

By mapping these consequences and the *app-score* in Matrix 2,

behavior-score = MAX (E, F, P, DC, LL, S, D)

= MAX (3, 2, 3, 3, 2, 2, 3) = 3

		Consequences																				
		E			F			P			DC			LL			S			D		
		L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
app-score	0	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
	1	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
	2	2	**3***	4	**2***	3	4	2	**3***	4	2	**3***	4	2*	3	4	2*	3	4	2	**3***	4
	3	3	4	5	3	4	5	3	4	5	3	4	5	3	4	5	3	4	5	3	4	5
	4	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6

B12.6 Based on findings of Chapter 4, the user-centric factor of conscientiousness personality trait has the most significant negative correlation with this behavior. Hence, according to the proposed model for calculating the significance correlation risk factor, *behavior-score* is recalculated independently for each user as follows:

IF conscientiousness = low THEN (Users A and D)

An opposite mapping will occur by mapping the user's conscientiousness group to high. In Matrix 3, the pre-calculated *behavior-score* = 3 is mapped to medium risk and *app-score* =2. Therefore, the resulting *behavior-score* = 5

Conscientiousness group		Low			High		
behavior-score		L	M	H	L	M	H
App-score	0	0	1	2	2	3	4
	1	1	2	3	3	4	5
	2	2	3	4	4	**5***	6
	3	3	4	5	5	6	7
	4	4	5	6	6	7	8

behavior-risk=AVG(*behavior-score*, *auth-score*, *connect-score*)+*account-type-score*

= AVG (5, 4, 4) +1 = 5.3

The final risk score/level, *Overall-risk* = (behavior-risk* W_{br})+ (system-risk *W_{sr})

where $W_{br=}$ W_{sr} = 0.5. Thus,

Overall-risk = (5.3 * 0.5) + (5.8 * 0.5) = **5.6 medium risk**

IF conscientiousness = high THEN (Users B, C and E)

An opposite mapping will occur by mapping the user's conscientiousness group to low. In Matrix 3, the pre-calculated *behavior-score* = 3 is mapped to medium risk and *app-score* =2. Therefore, the resulting *behavior-score* = 3

Conscientiousness group		Low			High		
behavior-score		L	M	H	L	M	H
App-score	0	0	1	2	2	3	4
	1	1	2	3	3	4	5
	2	2	**3***	4	4	5	6
	3	3	4	5	5	6	7
	4	4	5	6	6	7	8

behavior-risk=AVG(*behavior-score*, *auth-score*, *connect-score*)+*account-type-score*

= AVG (3, 4, 4) +1 = 4.7

The final risk score/level, *Overall-risk* = (behavior-risk* W_{br})+ (system-risk *W_{sr})

where $W_{br=}$ W_{sr} = 0.5. Thus,

Overall-risk = (4.7 * 0.5) + (5.8 * 0.5) = **5.3 medium risk**

The resulting risk scores/levels are as illustrated in Table 7.5.

Given that **Low** = 0 --- 3.9, **Medium** = 4 --- 6.9, **High** = 7 --- 10.

User	B1		B2		B3		B4		B5		B6		B7		B8		B9		B10		B11		B12	
	Sys-behavior-risk	Overall-risk	App-behavior-risk	Overall-risk	App-behavior-risk	Overall-risk	App-behavior-risk	Overall-risk	Sys-behavior-risk	Overall-risk	Sys-behavior-risk	Overall-risk	Sys-behavior-risk	Overall-risk	Sys-behavior-risk	Overall-risk	App-behavior-risk	Overall-risk	Sys-behavior-risk	Overall-risk	App-behavior-risk	Overall-risk	App-behavior-risk	Overall-risk
A	7.5	7.5	6.3	6.1	6.3	6.1	6	5.9	7.5	7.5	8.5	8.5	7.5	7.5	8	8	5	5.4	8.5	8.5	10	7.8	5.3	5.6
B	8.5	8.5	8.8	7.3	6	5.9	6.7	6.3	9.5	9.5	8.5	8.5	9.5	9.5	6	6	5.3	5.6	7.5	7.5	7.5	6.5	4.7	5.3
C	9.5	9.5	6.3	6.1	6.7	6.3	6	5.9	7.5	7.5	8.5	8.5	7.5	7.5	6	6	5.7	5.8	9.5	9.5	7.5	6.5	4.7	5.3
D*	9.5	9.5	8.8	7.3	6.7	6.3	6.7	6.3	9.5	9.5	8.5	8.5	9.5	9.5	8	8	5.7	5.8	9.5	9.5	10	7.8	5.3	5.6
E**	7.5	7.5	6.3	6.1	6	5.9	6	5.9	7.5	7.5	8.5	8.5	7.5	7.5	6	6	5	5.4	7.5	7.5	7.5	6.5	4.7	5.3

Table 7.5: The Resulting Users' Risk Profiles

*user with highest risk profile , **user with lowest risk profile.

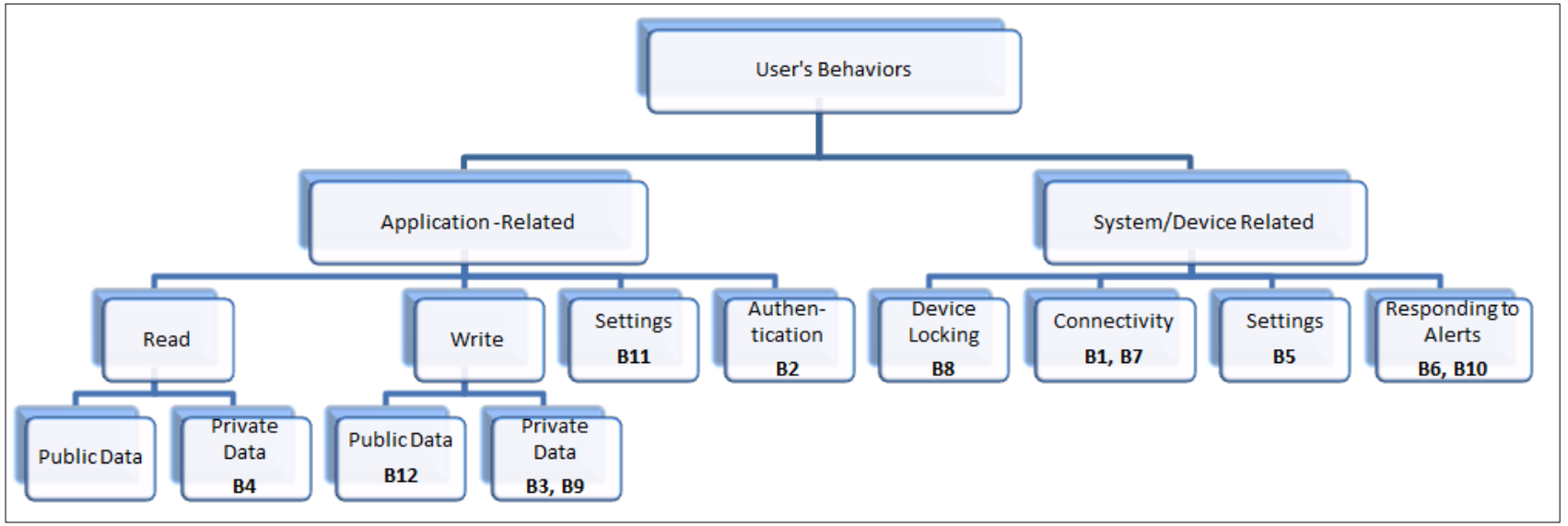

Figure 7.10: A Mapping of The Suggested Categorization of Behaviors to Simulation's Behaviors (B#)

A comparison of these results based on the impact of user-centric factors on the resulting risk scores/levels, highlights a similar trend to that obtained from Experiments I and II. As IT proficiency and conscientiousness personality trait user-centric factors were found to be most significantly negatively correlated with behaviors B2, B4 and B5 for the former and behaviors B8, B11 and B12 for the latter, this impact is explicit. IT professionals and those with a high level of conscientiousness personality trait were in lower risk than non-IT professionals and users with lower levels of conscientiousness as in Figures 7.11 and 7.12. A similar impact was apparent for males over females as gender user-centric factor is most significantly negatively correlated with behavior B7 as in Figure 7.13.

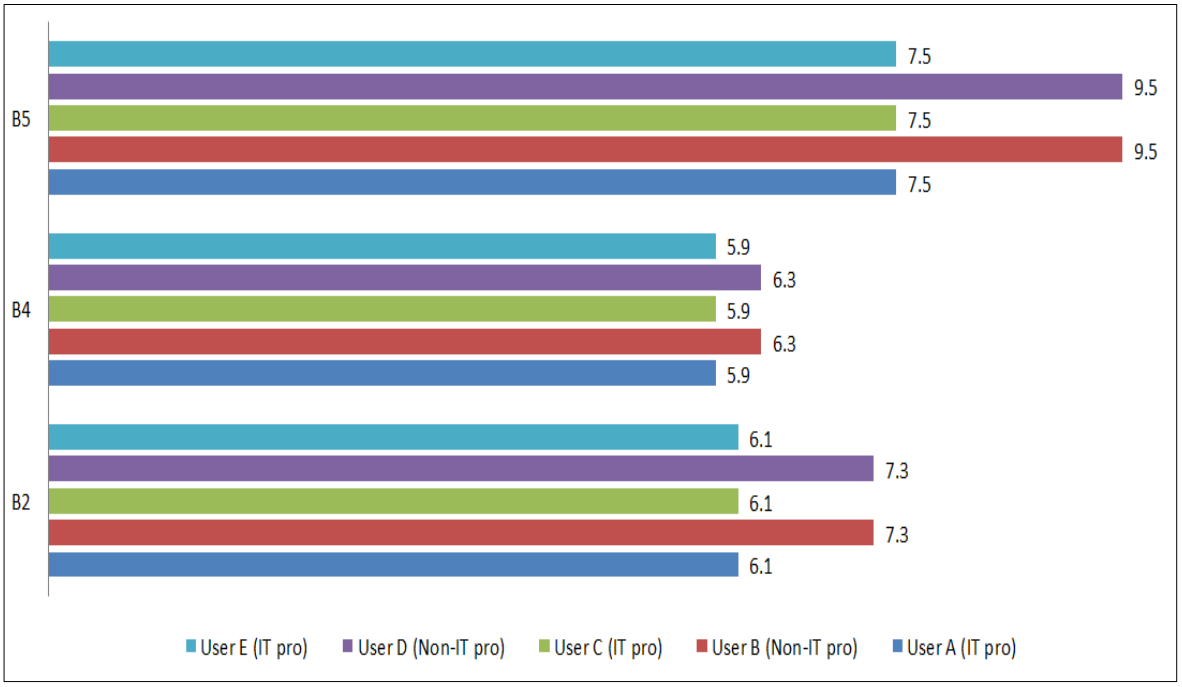

Figure 7.11: Impact of IT Proficiency user-centric Factor on Behaviors B2, B4 and B5

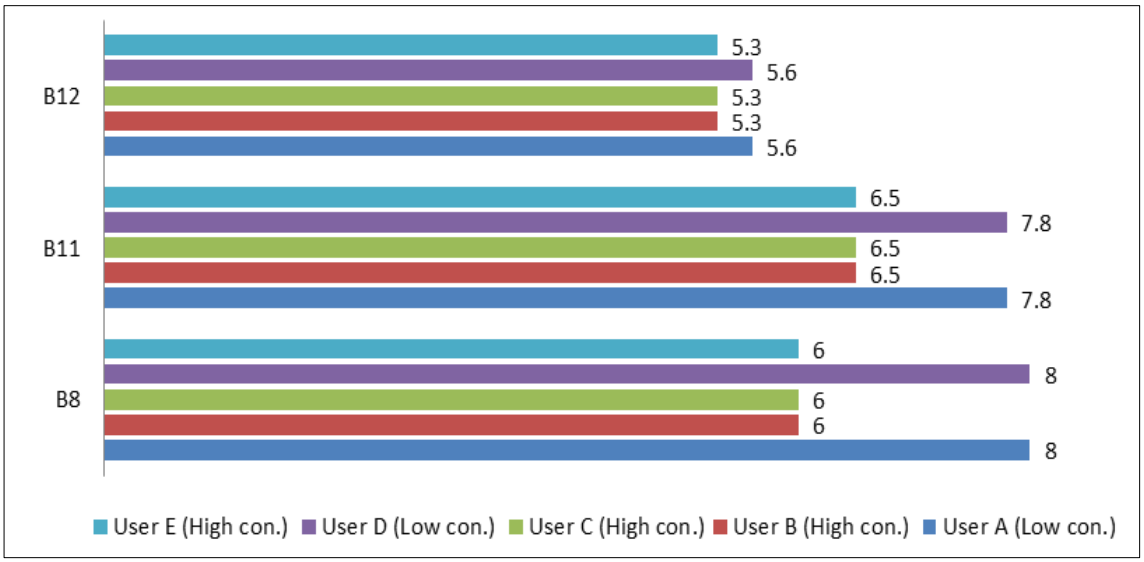

Figure 7.12: Impact of Conscientiousness Personality Trait User-centric Factor on Behaviors B8, B11 and B12

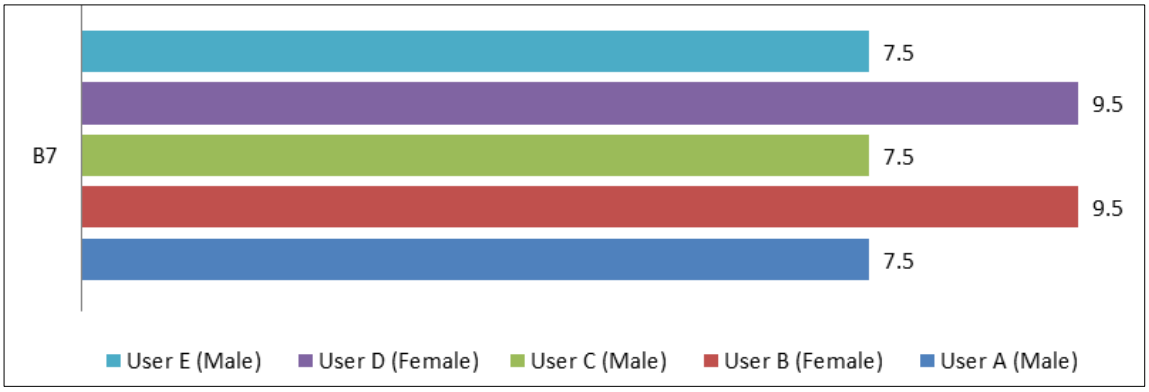

Figure 7.13: Impact of Gender User-centric Factor on Behavior B7

The user-centric factors of age and service usage levels are categorized in three levels of low, medium and high with an opposing significant correlation with behaviors B1 and B9 for the former and B3 and B10 for the latter. As illustrated in Figures 7.14 and 7.15, the variations in these user-centric factors resulted in varying risk profiles for users as the higher the service usage level of the user the higher the risk and conversely, the older the user the lower his risk level.

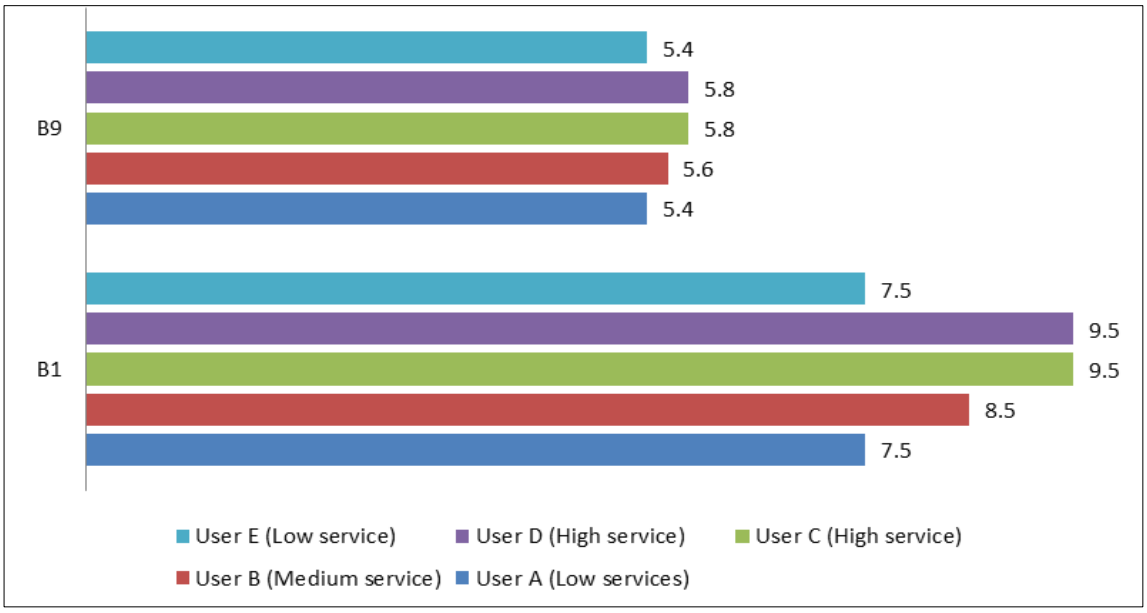

Figure 7.14: Impact of Service usage User-centric Factor on Behaviors B1 and B9

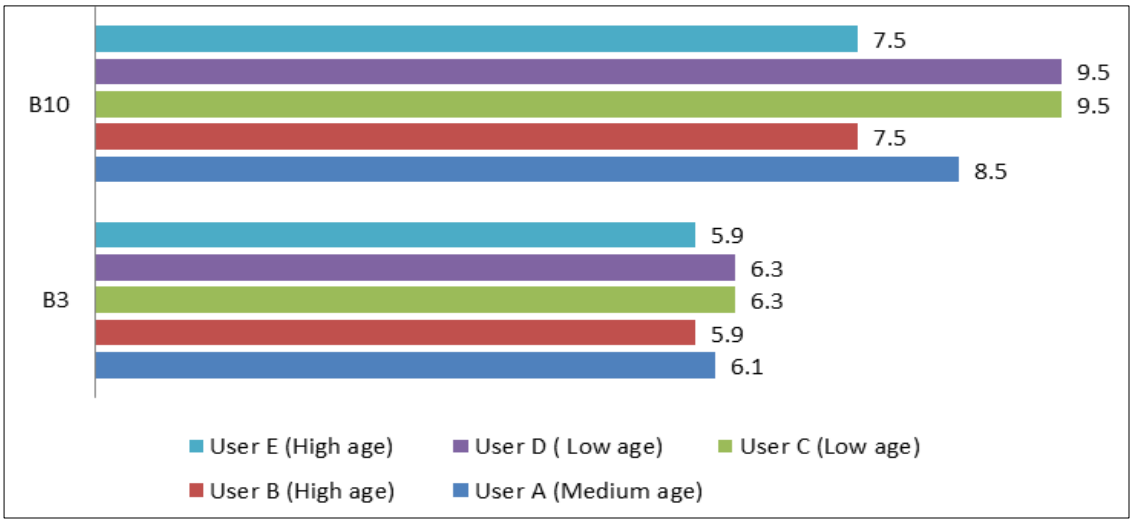

Figure 7.15: Impact of Age User-centric Factor on Behaviors B3 and B10

Opposing to the above mentioned behaviors resulting risk scores/levels, behavior B6 that was found not to be significantly correlated with any of the studied user-centric factors resulted in a unified risk score/level, i.e. 8.5 High risk, for all users as in Figure 7.16. The comparison between resulting risk scores/levels of other behaviors and those of behavior B6 serve to show how the proposed risk models take into account the variations in the most significant correlated user-centric

factors when calculating risk. Moreover, it shows that for the same behavior, different risk scores were obtained based upon the differences in user's user-centric factors highlighting the difference between an individualized and non-individualized risk score/level.

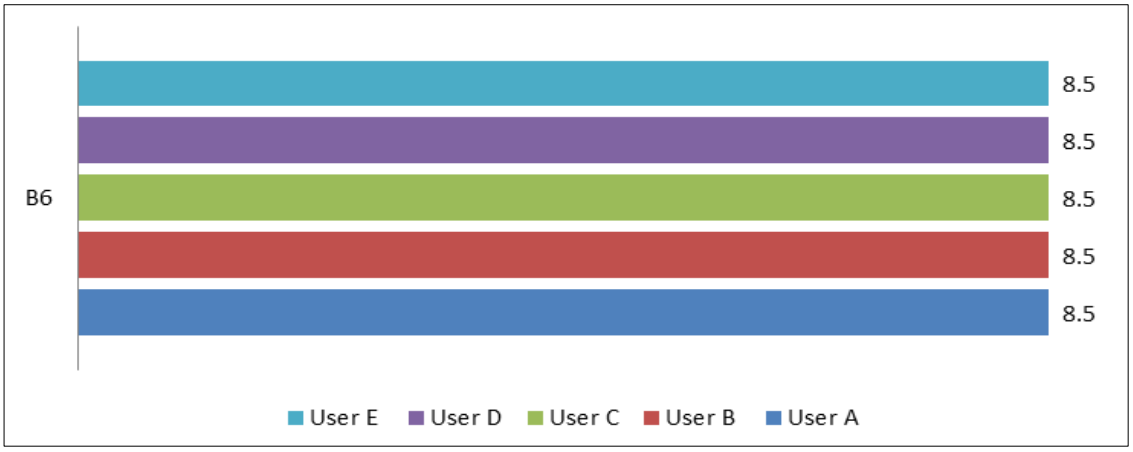

Figure 7.16: Impact of Non Significance Correlation on Behavior B6

This simulation is based on a time line scenario of activities. To reflect the evolving nature of risk over time, Figure 7.17 illustrates how the risk score changes for each user as the time goes through the scenario based upon the behaviors being exhibited.

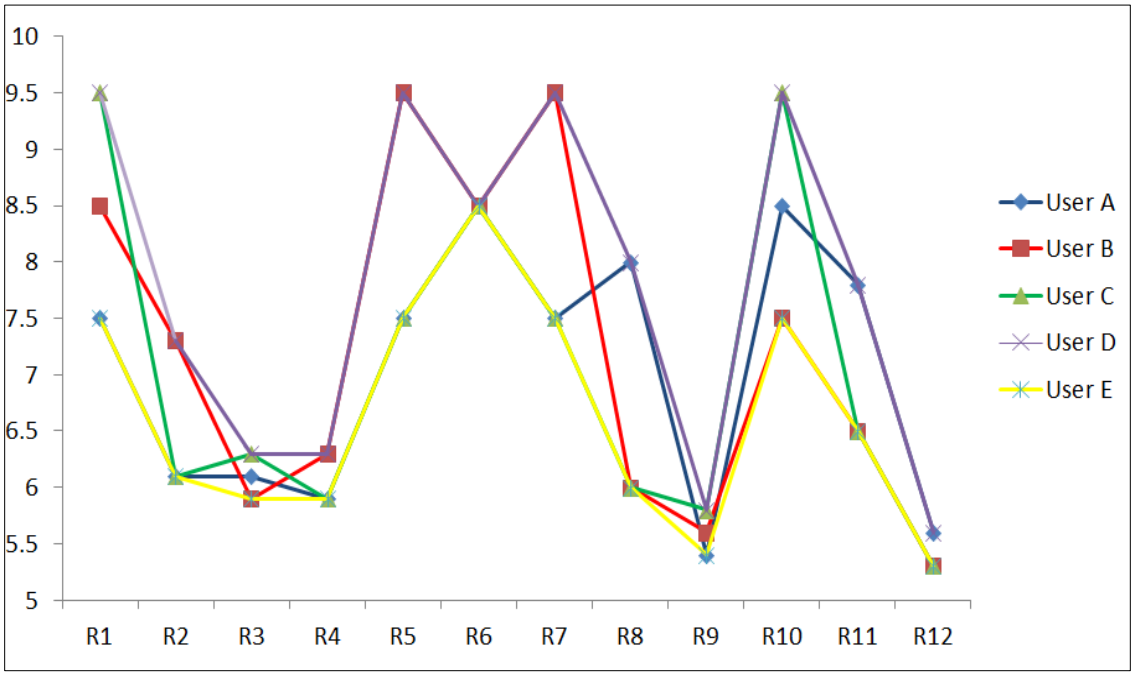

Figure 7.17: Resulting Users' Risk Profiles Over Time

7.4 Discussion

The findings of Chapter 4 were employed in proposing a User-centric Risk Assessment Model that takes into account, when calculating risk, variations in user's characteristics. In addition, other behavioral-related factors were considered resulting in a risk score/level not of a single behavior but of compound risk. Using two experiments and a scenario-based simulation of a variety of users with different risk profiles, the proposed risk calculation models were applied and results analyzed. It was an opportunity to show that risk has to be based on the user and there are factors whether user-centric or behavioral-related that influence his behavior. This is evident as different risk profiles were obtained for the same behavior as a result of variations in users'-centric factors such as his age, personality trait and service level usage showing that the proposed models can adapt to change in these factors to produce an individualized risk score/level.

The resulting risk scores/levels of simulation as in Table 7.5, reflect the noted trends and patterns from Experiments I and II. However, when comparing the resulting risk scores/levels of a certain behavior for different users, as in B4 for instance, we are able to see no difference in the risk level. From the user's perspective, this increase or decrease in the risk score but within the same risk level may not be relevant. Consequently, the nature of the proposed models do not allow for a decrease or an increase of 3, for instance, in one hit. Thus, this level of granularity is picked up and understood by the security response manager that this 0.7 increase or decrease, for example, does mean something and acts accordingly. This is similar in concept to the concept of "Fever" in the human body. As the normal temperature is 37.5°c, an increase of temperature of 0.30°c to 37.8° implies that the person has high fever and a medical procedure has to be applied. Similarly, the temperature of 39°c is still considered high fever but the difference is in how it is treated.

Moreover, the analysis showed that, based on proposed models, user's risk level is not primarily impacted by a change in a statistically significant user-centric factor only, but also by a change in a number of behavioral-related factors. Actually, the resulting risk scores/levels either

decreased or increased as a consequence of change in these factors and a number of general trends were identified. Among those behavioral-related factors were password hygiene in terms of *auth-score* variable and type of used communication medium in terms of *connect-score* variable.

Unlike application-related behaviors where several factors are considered when calculating risk scores, only user-centric factors are considered when calculating risk for system-related behaviors. As such, the impact of a statistically significant user-centric factor and the contribution of behavioral-related factors such as *auth-score* and *connect-score* as standalone behaviors to both *behavior-risk* or *overall-risk* were more obvious.

When analyzing the impact of the user-centric factor of IT proficiency on the resulting *behavior-risk* and *overall-risk* on behavior B2 of simulation (Using the same password for multiple sensitive accounts), for example, the behavioral-related factor of authentication thru *auth-score* is the primary behavioral-related factor used when calculating *behavior-risk*. When comparing the resulting *behavior-risk* of this behavior, and consequently the resulting *overall-risk*, with another application-related behavior that has significant negative correlation with IT proficiency such as the application-related behavior read private data of "clicking on attachments/links in an email from a friend without checking" (as in behavior B4 in simulation), the impact of IT proficiency is more apparent as in Table 7.6. The *behavior-risk* of B2 is 6.3 for IT professionals and 8.8 for non-IT professionals compared to 6 for IT professionals and 6.7 for non-IT professionals in B4.

Moreover, when analyzing the impact of the user-centric factor of service usage on the resulting *behavior-risk* and *overall-risk* on behavior B1of simulation (Connecting to public WiFi), for example, the behavioral-related factor of used communication medium thru *connect-score* is the primary behavioral-related factor used when calculating *behavior-risk*. When comparing the resulting *behavior-risk* of this behavior, and consequently the resulting *overall-risk*, with another application-related behavior that has significant positive correlation with service usage such as the

application-related behavior write private data of "allowing web browsers to remember passwords" (as in behavior B9 in simulation), the impact of service usage is more apparent on B1 as a standalone behavior than on B9 as in Table 7.7. *Behavior-risk* level was high with scores of 7.5, 8.5, and 9.5 for service usage levels of low, medium and high in B1 whereas it is medium level with scores of 5, 5.3 and 5.7 in B9 for service usage levels of low, medium and high. This suggests a stronger impact of a user-centric factor on resulting risk scores/levels than when combined with other factors.

	"Using the same password for multiple sensitive accounts", B 2		**"Opening/clicking on links/attachments in emails from friends without checking", B4**	
IT proficiency	***behavior-risk***	***Overall-risk***	***behavior-risk***	***Overall-risk***
IT professionals	6.3	6.1	6	5.9
Non-IT professionals	8.8	7.3	6.7	6.3

Table 7.6: Impact of IT proficiency on Resulting Risk Scores/Levels

	"Connecting to a public WiFi", B 1		**"Allowing web browsers to remember password", B9**	
Service usage level	***behavior-risk***	***Overall-risk***	***behavior-risk***	***Overall-risk***
Low	7.5	7.5	5	5.4
Medium	8.5	8.5	5.3	5.6
High	9.5	9.5	5.7	5.8

Table 7.7: Impact of Service Usage Level on Resulting Risk Scores/Levels

To this end, the proposed scale from 0 to 10 is not a definitive scale but it allows a level of granularity of risk. These examples serve to demonstrate that user-centric factors do contribute to the resulting risk scores/levels either by escalating or deescalating it, but this amount of contribution is not fixed for all behaviors. There is clear evidence to suggest that risk factors are changing based upon behavior and that, in comparison to prior work, the proposed approach

incorporating user-centric factors in calculating risk is a novel approach to information security risk assessment.

7.5 Conclusion

There are other sources of risk, i.e. threats, to the user other than his actual behavior. These sources range from user-centric to behavioral-related. Using three experiments, the proposed user-centric risk calculation models were tested for calculating both *behavior-risk* and *overall-risk* and results analyzed. The proposed risk calculation models worked in the way they were expected to. The analysis of results revealed a number of trends and relations. Further to that, the analysis provided evidence that the level of impact and contribution of such factors is not fixed for all users and behaviors. This being said, their impact was stronger when used as standalone behaviors. Aside from the "*one size fits all*" solution, encouragingly, the results of these experiments provided an indication that risk could be assessed differently for the same behavior based on a number of user-centric and behavioral-related factors resulting in an individualized risk score/level.

Chapter 8 : Conclusions and Future Work

This chapter concludes this research and highlights the achievements, limitations and opportunities for future work. This research aimed at developing a novel approach to individually and adaptively assessing and communicating risks focusing specifically on factors such as user behavior, awareness, and timeliness.

8.1 Achievements of Research

The research objectives stated in Chapter 1were met through the following achievements:

1. **Developed a current state-of-the-art understanding of Information Security Risk Assessment methods.** The literature review in Chapter 2 discussed and analyzed various information security risk assessment methodologies and approaches. Firstly, those tailored for organizations were classified according to a suggested classification approach then analyzed. Additionally, enhancements to such methodologies were demonstrated. Secondly, information security risk assessment methodologies intended for users of the general public were presented discussing both their advantages and disadvantages. This provided an overview of some of the challenges and key issues related to information security risk assessment.
2. **Investigated the current approaches in security awareness, usability and human aspects of information security**. This was achieved using a systematic literature review as in Chapter 3. The literature indicated that users have problems in protecting themselves due to various issues such as lack of awareness and usability problems. As human's behavior is one of the causes of information security problems, information security awareness aims to improve that behavior. However, when discussing and analyzing the current approaches to information security awareness, it has been found that they rely mostly on the one-size-fits-all approach that needs to be improved.

3. **Identified the factors that influence user's risk taking behavior.** The literature review in Chapter 3 also indicated that some users tend to be *at-risk* more than others, therefore, risk is not the same for all users. This is due to several factors that impact his behavior. The chapter concluded by outlining these factors and explaining how they contribute to the risk level of user's behaviors. These influencers range between demographic to psychological and risk communication/awareness factors.
4. **Explored the extent in which users are making risk informed decisions.** This was achieved using an online user survey as explained in Chapter 4. The analysis of the survey results demonstrated that users use more than one device with different platforms to perform their daily activities which increases the burden upon them in maintaining security across different devices and applications. Moreover, a holistic view of user's risk-appetite was explored from several aspects including data management and authentication. The analysis of such behaviors suggested that users do consider information security to be important and practice a baseline of security knowledge that requires considerable improvement.
5. **Analyzed the relationship between differences in users' characteristics (user-centric factors) and their risk-taking behavior**. Being that several factors were identified to influence user's security behaviors, the survey in Chapter 4 also investigated the relationship between user-centric factors and user's behaviors. Using Pearson Correlation, the set of analysis across a set of factors and behaviors provided a more appreciated understanding of what significant relations exist. Therefore, considering them when assessing and responding to user's risks will result in a more realistic and individualized risk assessment and communication.
6. **Proposed a novel model for User-centric Risk Assessment and Response (UCRAR) that assesses risks on both user and system level and generate an individualized risk profile accordingly.** Capitalizing upon the knowledge gained, a novel model was proposed

in Chapter 5 that aimed at enhancing user's security behavior. The model is intended to provide a comprehensive framework for individually, continuously and timely assessing and communicating information security risks. The novelty of the proposed model depends upon four significant aspects: the continuous monitoring of user's behaviors, an aggregated risk score/level based upon risk assessment on both the user and system level, an individualized risk profile and a persuasive individualized response mechanism. These aspects are utilized to enhance user's risk taking behavior and transform him from being ill-informed to a security minded user who is able to make a risk informed decision.

7. **Developed a novel approach in security awareness and usability to communicate risks effectively to users by designing a communication that efficiently and individually interacts with users.** Based on the analysis of the generated individualized risk profile, a decision is made on how to best communicate and educate the user about his behavior as explained in Chapter 5. The novelty of this approach is that, aside from the traditional one-message/one-size-fits-all approach, several factors are considered when deciding how to respond to user's behavior. Examples of such factors are the risk score/level, has the behavior been undertaken before or not and the time period between these behaviors. As part of its novelty, the user is persuasively and individually educated about his risk taking behavior using a gradual response mechanism where response severity is escalated from level 1 to level 6 and by utilizing three response approaches. Moreover, user-centric factors and learning styles are considered among other factors in this mechanism.
8. **Proposed novel risk models that adapts to user's-centric factors when calculating both of system and user level risks and generates an aggregated risk.** As UCRAR provided an understanding of both user and system based risk, a novel mechanism for estimating such risks is proposed in Chapter 6. Aside from the traditional risk assessment formula, three risk estimation models are proposed: a user-centric, system-based and an aggregated model. As part of its novelty, both user-centric and behavioral-related factors

are considered. This resulted in an individualized near real-time risk assessment in granular form.

9. **Designed and implemented a scenario based simulation from which the models will operate.** This involved various users with different combinations of user-centric factors to evaluate the effectiveness, reliability and feasibility of the proposed approach as in Chapter 7. According to the proposed model, risks were assessed and results analyzed for each user/behavior. The analysis of simulation results was useful in demonstrating how risk is not the same for all users and how the proposed model is effective in adapting to differences between users.

8.2 Limitations of The Research

Although the research objectives were met, a number of limitations can be identified. The key limitations of this research are as follows:

1. With regards to the research nature, an implementation of the proposed model in a real environment was challenging especially that this research was conducted by a single researcher with limited timeframe and resources. Hence, a better understanding of its effectiveness could be given by implementing and evaluating the proposed model in practical sense across a population of users.
2. Only one risk assessment model was used, i.e. matrix-based. This was largely built upon best-practices. However, the literature has identified a variety of risk models that could be used.
3. Whilst the survey conducted provided a holistic perspective of user's risk-taking behavior from multiple domains, having more behaviors and more factors would have provided a richer and a more comprehensive set of analysis.
4. How user-centric and system-based risk contribute to final risk score/level has not been investigated. Similarly, the impact of operating system, application vulnerability/risk and

network risk on the system-based risk score/level. Therefore these issues need to be considered to provide a more realistic assessment.

5. The consideration of installed security software and its functionality was outside the scope of this research. Although the Risk Communication component of UCRAR does consider this in terms of registering messages delivered by such software, but this was not the case in the risk assessment component. The consideration of this will result in a better understanding of risk.

8.3 Future Work

A number of areas and opportunities exist for further enhancement and research. These are as follows:

1. A complete fully functional version of the proposed model need to be developed and implemented in a real environment. This will be helpful in understanding the effectiveness of the model in enhancing user's security behavior. Additionally, this will facilitate model's evaluation and finding any limitations.
2. The design of an experiment that can empirically understand and measure the relationship between user-centric risk assessment and system-based risk assessment and their proportion of impact on final risk score/level. So as the impact of operating system, application and network router (if any) vulnerability on system-based risk.
3. Further investigation of different risk assessment models aided by a practical evaluation by getting real user data in. This will give an opportunity to a better understanding of which is the most effective and the granularity of generated risk scores/levels.
4. Users use more than one device for performing their activities. Having the proposed model running on multiple devices, behaviors are monitored and assessed on them simultaneously as one assessment instead of assessing behaviors on each device separately. This will strengthen the enhancement of user's security behavior.

5. When assessing user's behavior, more than one user-centric factor could be considered and not only the factor with the most significant correlation. This will enhance the individualized level of the resulting risk scores/levels. Moreover, the assessment is not limited to only one insecure behavior but to a number of behaviors, i.e. compound risk.
6. The consideration of installed security software and its functionality in the risk assessment.
7. The design and implementation of the processes proposed in UCRAR such as the Good behavior repository, the community-based risk data. Additionally, the implementation and evaluation of the Risk Communication component. Altogether, this will result in a complete implementation of the proposed model.

8.4 The Future of Information Security Risk Assessment

Carrying on daily activities using services provided by computing devices and the Internet are becoming part of users' daily life. With this increase use, comes an increase in information security threats that users are not well aware of and not well equipped to protect themselves against the continuously evolving threat landscape. Although many methodologies exist for information security risk assessment, this research highlights the need to go beyond the traditional mechanisms to a continuous, timely and individualized assessment. In this research, a model has been proposed in which understanding risks posed to users is achieved by focusing on their behaviors and how to improve it. However, there is a wider set of issues in terms of better understanding the nature of the behavior, how the behavior changes over time, the evolution of those behaviors, how user-centric factors change over time and how that information could be better used within wider issues of information security awareness, education and communication. Moreover, the existing literature is largely about behavioral intent, the research domain needs to explore opportunities for developing new mechanisms to actually measure the behavior itself rather than behavior intent. Not specifically to the proposed model, but taking these concepts and applying them to information

security risk assessment, awareness, education and training such that the more that is done in that domain, the more secured individuals and behaviors will result.

Appendix A: End-users' Survey Questions (Clarke et al. 2016)

SECTION A: Demographics

A.Q1: Please select the appropriate age group in which you belong:

○ 18-25 ○ 26-30 ○ 31-35 ○ 36-40 ○ 41-45 ○ 46-50 ○ 51-55
○ 56-60 ○ 61+

A.Q2: Please select your gender:

○ Female ○ Male

A.Q3: In which country do you reside:

A list of Countries

A.Q4: Please select your highest level of education:

○ Secondary School (e.g. GCSE) ○ Higher Education (e.g. Bachelor's degree, MSc, PhD) ○ Further Education (e.g. A-level)

A.Q5: Are you a student:

○ Yes ○ No

A.Q6: What is your occupation:

○ Education, training, and library occupations ○ Office and administrative support occupations ○ Healthcare practitioners and technical occupations ○ Management occupations ○ Business and financial operations occupations
○ Computer and mathematical occupations ○ Healthcare support occupations ○ Community and social services occupations ○ Protective service occupations ○ Life, physical, and social science occupations
○ Building and grounds cleaning and maintenance occupations ○ Arts, design, entertainment, sports, and media occupations

A.Q7: Which subject do you study:

○ Social Work ○ Politics ○ Mathematics ○ Computing & IT ○ Veterinary Medicine ○ Sociology ○ Law
○ Biology ○ Music ○ Communication and Media ○ Geography ○ Philosophy ○ Music
○ Earth Sciences ○ Engineering ○ English Literature ○ Education ○ Economics ○ Chemistry ○ History
○ Dentistry ○ Psychology and Counselling ○ Management ○ Health and Medicine ○ Accounting, Business & Finance

SECTION B: IT Background

B.Q1: How would you rate your IT proficiency- (1 Novice, 3 Experienced and 5 Expert)

○ 1 ○ 2 ○ 3 ○ 4 ○ 5

B.Q2: Which of the following digital devices do you use- (Select all that apply)

○ Android Tablet/Smartphone (e.g. Samsung Galaxy Tab, HTC)
○ BlackBerry Tablet/Smartphone (e.g. BlackBerry PlayBook, Q10)
○ Game Console
○ GPS/Navigation Device
○ Handheld Game Console
○ iPad/iPad mini/iPhone
○ Linux Desktop/Laptop
○ Mac Desktop/Laptop
○ Smart TV
○ Smart Watch
○ Windows Desktop/Laptop
○ Windows Tablet/Smartphone (e.g. Microsoft Surface, Nokia Lumia)
○ Other

B.Q3: How frequent do you engage in the following services:

	Always	Often	Sometimes	Rarely	Never
1. Access Emails (e.g. Gmail)	○	○	○	○	○
2. Cloud services (e.g. Dropbox)	○	○	○	○	○
3. Information gathering (e.g. reading news, weather forecast)	○	○	○	○	○
4. Instant messenger (e.g. Skype, WhatsApp)	○	○	○	○	○
5. Online banking	○	○	○	○	○
6. Online blogs/forums	○	○	○	○	○
7. Online gaming	○	○	○	○	○
8. Online shopping (e.g. Amazon)	○	○	○	○	○
9. Peer to peer sharing (e.g. torrents)	○	○	○	○	○
10. Social networking (e.g. Facebook, LinkedIn)	○	○	○	○	○
11. Watch TV or video (e.g. BBC iPlayer, YouTube)	○	○	○	○	○
12. Word processing and Spreadsheet (e.g. Microsoft Office)	○	○	○	○	○

SECTION C: IT Security Practice

C.Q1: How high a priority is IT security for you:

○ Essential ○ High priority ○ Medium priority ○ Low priority ○ Not a priority

C.Q2: Which of the following do you use on your computing devices

○ Anti-virus software / Internet Security Suites ○ Anti-spam software ○ Biometrics (e.g. facial recognition, fingerprint) ○ Data backup ○ Graphical passwords (e.g. Windows 8) ○ Firewall

○ Intrusion Detection System ○ Intrusion Attacking System ○ Pattern locks (e.g. Android) ○ Secret knowledge (e.g. PIN / password) ○ Encryption ○ Other

C.Q3: How many passwords do you have (including both devices and services (e.g. Amazon, eBay)):

○ 1-5 ○ 6-10 ○ 11-15 ○ 16-20 ○ 21-25 ○ 26+

C.Q4: What proportion of your passwords can be described by the following statements:

	0-40%	41-80%	81-100%
1. Contains alphabetic characters	○	○	○
2. Contains lower case characters	○	○	○
3. Contains upper case characters	○	○	○
4. Contains numbers	○	○	○
5. Contains punctuation symbols	○	○	○
6. Has been recycled / reused	○	○	○
7. Is 8 characters or more	○	○	○

C.Q5: Typically, how often do you change your passwords:

○ Less than 3 months ○ Between 3-6 months ○ Between 7-12 months ○ More than 1 year ○ Whenever a system requires me to do so ○ Never

C.Q6: What kind of information do you share on social networking websites (e.g. Facebook, Twitter, LinkedIn etc.):

○ Name ○ Date of birth ○ Postal address ○ Email address ○ Telephone ○ Pictures of family and friends

○ Information of family and friends ○ Other

C.Q7: Have you experienced any of the following security incidents:

○ Data loss ○ Denial of Service ○ Trojan ○ Hardware failure ○ Phishing ○ Phibbing ○ Spyware

○ Device loss (e.g. mobile phone/ USB / security token) ○ Malware (e.g. virus, worm) infection ○ Unauthorised access ○ Whooping ○ Other

C.Q8: Please indicate how frequently the following statements apply to you:

	Always	Often	Sometimes	Rarely	Never
1. I share my password with others	○	○	○	○	○
2. I lock my workstation when I am away from my desk	○	○	○	○	○
3. I store my passwords	○	○	○	○	○
4. I click on links / attachments within an email from unknown sources	○	○	○	○	○
5. I click on links / attachments within an email from friends/colleagues without checking	○	○	○	○	○
6. I connect to a public wireless network (e.g. Starbucks Wi-Fi)	○	○	○	○	○
7. I disable wireless technologies (e.g. Wi-Fi, Bluetooth) on my laptop/tablet/mobile)	○	○	○	○	○
8. I delete suspicious emails	○	○	○	○	○
9. I notify IT support when I receive suspicious emails	○	○	○	○	○
10. I use an encrypted USB drive to transfer files between computers	○	○	○	○	○
11. I keep my anti-virus software up-to-date	○	○	○	○	○
12. I scan a USB drive before using it	○	○	○	○	○
13. I back-up my data files on a regular basis	○	○	○	○	○
14. I use a password to log-in my home computer system	○	○	○	○	○
15. I insert & access USB sticks/CD/DVD from unknown sources	○	○	○	○	○
16. I encrypt sensitive information on my computer	○	○	○	○	○
17. I destroy all data before disposing of hardware (e.g. laptop, mobile phones)	○	○	○	○	○
18. I install the latest security patches for my Operating System/ software applications/ web browsers without any delay	○	○	○	○	○
19. I download files from suspicious/unknown websites	○	○	○	○	○
20. I accept invitations from people I do not know on social networking websites	○	○	○	○	○
21. I use a same password for multiple sensitive accounts	○	○	○	○	○
22. I install/use pirate software on my computing devices	○	○	○	○	○
23. I disable antivirus /firewall (e.g.	○	○	○	○	○

because it was slowing down my computer)					
24. I cancel or postpone a security related software update	○	○	○	○	○
25. I allow web browsers/systems/applications to remember my passwords	○	○	○	○	○
26. I open a document despite security warnings	○	○	○	○	○
27. I forward chain emails (e.g. if you forward this email 50 times and you will be healthier)	○	○	○	○	○
28. I use an anonymising proxy	○	○	○	○	○
29. I use a VPN (Virtual Private Network)	○	○	○	○	○
30. I use a TOR (The Onion Router) network	○	○	○	○	○
31. I ensure I log off from online systems (e.g. Facebook account) before closing the browser/app	○	○	○	○	○

C.Q9: Which of the following channels have you proactively used to enhance your knowledge of IT security:

○ Internet ○ A colleague ○ IT Support Officer ○ Information security literature ○ Training Course ○ Never / Not interested
○ Haven't to date, but would like to learn more ○ Other

SECTION D: PERSONALITY TRAITS

D.Q1: Please indicate to what extent you agree or disagree that these personal characteristics describe you:

	Strongly Agree	Agree a little	Neither agree nor disagree	Disagree a little	Strongly disagree
1. Is talkative	○	○	○	○	○
2. Tends to find fault with others	○	○	○	○	○
3. Does a thorough job	○	○	○	○	○
4. Is depressed, blue	○	○	○	○	○
5. Is original, comes up with new ideas	○	○	○	○	○
6. Is reserved	○	○	○	○	○
7. Is helpful and unselfish with others	○	○	○	○	○
8. Can be somewhat careless	○	○	○	○	○
9. Is relaxed, handles stress well	○	○	○	○	○
10. Is curious about many different things	○	○	○	○	○

11. Is full of energy	○	○	○	○	○
12. Starts quarrels with others	○	○	○	○	○
13. Is a reliable worker	○	○	○	○	○
14. Can be tense	○	○	○	○	○
15. Is ingenious, a deep thinker	○	○	○	○	○
16. Generates a lot of enthusiasm	○	○	○	○	○
17. Has a forgiving nature	○	○	○	○	○
18. Tends to be disorganized	○	○	○	○	○
19. Worries a lot	○	○	○	○	○
20. Has an active imagination	○	○	○	○	○
21. Tends to be quiet	○	○	○	○	○
22. Is generally trusting	○	○	○	○	○
23. Tends to be lazy	○	○	○	○	○
24. Is emotionally stable, not easily upset	○	○	○	○	○
25. Is inventive	○	○	○	○	○
26. Has an assertive personality	○	○	○	○	○
27. Can be cold and aloof	○	○	○	○	○
28. Perseveres until the task is finished	○	○	○	○	○
29. Can be moody	○	○	○	○	○
30. Values artistic, aesthetic experiences	○	○	○	○	○
31. Is sometimes shy, inhibited	○	○	○	○	○
32. Is considerate and kind to almost everyone	○	○	○	○	○
33. Does things efficiently	○	○	○	○	○
34. Remains calm in tense situations	○	○	○	○	○
35. Prefers work that is routine	○	○	○	○	○
36. Is outgoing, sociable	○	○	○	○	○
37. Is sometimes rude to others	○	○	○	○	○
38. Makes plans and follows through with them	○	○	○	○	○
39. Gets nervous easily	○	○	○	○	○
40. Likes to reflect, play with ideas	○	○	○	○	○
41. Has few artistic interests	○	○	○	○	○
42. Likes to cooperate with others	○	○	○	○	○
43. Is easily distracted	○	○	○	○	○
44. Is sophisticated in art, music, or literature	○	○	○	○	○

Appendix B: Significance Testing on The Relationship Between User-centric Factors and The Risk Taking Behavior Using Pearson's Chi-square Test

*** Null hypothesis is rejected for this factor/behavior due to strong evidence against it (p-value < 0.05), ** Changed risk level from Sample**

I.Password Hygiene Behaviors	Risk Level	Percentage (%)														
		Sample	IT proficiency			Age (in years)				Gender			Service Usage			
			IT pro	Non-IT pro	p-value	18-30	31-50	51+	p-value	Male	Female	p-value	High	Medium	Low	p-value
I.1 Changing of passwords	H	63	56	68	0. 06638	66	59	52	0. 082159	60	69	0.06799	56	65	65	0.09673
	M	32	40	24		32	32	33		34	27		41	31	26	
	L	6	4	7		3	10	15		6	4		3	4	9	
I.2 Sharing of Passwords	H	10	3	16	**1.25E-06***	11	9	11	0.34436	7	18	**9.90E-05***	9	8	13	0.39704
	M	28	28	29		31	25	19		27	32		26	32	27	
	L	62	69	55		58	66	70		66	50		65	60	60	
I.3 Storing of passwords	H	43	37	48	**0.00711***	41	44	52	0.65054	40	50	**0.04770***	44	37	47	0.45584
	M	22	21	22		23	21	11		23	21		22	24	20	
	L	36	**42	30		36	35	37		38	30		34	**39	33	
I.4 Using the same password for multiple accounts	H	63	55	70	**0.00138***	70	53	48	**1.74E-05***	62	67	0.40849	61	68	61	0.16810
	M	17	21	14		16	21	7		17	17		20	16	17	
	L	20	24	16		14	26	44		21	16		20	16	22	
I.5 Web-browsers/systems/ applications to remember password	H	61	62	60	0.78079	68	52	26	**1.51E-05***	63	56	0.12045	71	64	50	**0.00030***
	M	18	18	17		15	23	26		16	23		16	16	21	
	L	22	20	23		18	25	**48		22	21		13	20	30	
I.6 Locking workstation when away from desk	H	31	29	32	**0.00382***	34	25	19	**0.04638***	32	28	0.73038	21	33	36	**0.00165***
	M	25	28	23		26	26	19		25	26		23	30	24	
	L	44	43	45		40	48	63		43	46		56	37	40	
I.7. Using a password to log in home computer	H	23	15	29	0.10592	24	21	11	0.19472	21	28	0.15389	16	20	30	0.23409
	M	12	10	14		10	16	11		13	10		9	13	14	
	L	60	74	57		65	63	78		66	63		75	67	55	
I.8. Logging off from online systems before closing the browser/app	H	56	52	60	0.18556	59	55	26	**0.02173***	55	60	0.50126	55	62	52	0.28175
	M	20	22	19		20	22	19		20	20		18	19	23	
	L	24	26	21		21	23	**56		25	21		27	19	25	

I.Password Hygiene Behaviors	Risk Level	Percentage (%)														
		Openness			Conscientiousness			Extraversion			Agreeableness			Neuroticism		
		BFI+	BFI-	p-value	BFI+	BFI-	p-value	BFI+	BFI-	p-value	BFI+	BFI-	p-value	BFI+	BFI-	p-value
I.1 Changing of passwords	H	79	69	0.07594	60	73	0.27539	61	**64**	0.75232	62	65	0.64823	66	61	0.07488
	M	16	22		34	23		33	31		32	31		32	32	
	L	5	9		6	4		6	5		6	4		2	8	
I.2 Sharing of Passwords	H	9	16	0.16503	8	19	**0.00030***	12	8	**0.04630***	10	**13**	0.34478	11	10	0.53742
	M	28	29		28	30		30	27		30	**23**		30	27	
	L	63	56		65	50		58	66		61	64		58	63	
I.3 Storing of passwords	H	42	46	**0.03155***	44	38	0.10544	45	39	0.11216	42	45	0.05136	42	43	0.93393
	M	20	33		20	29		19	26		20	31		21	22	
	L	38	21		36	33		36	34		38	24		36	35	
I.4 Using the same password for multiple accounts	H	61	72	**0.03199***	59	76	**0.00301***	64	**63**	0.24265	63	62	0.47600	70	60	**0.04672***
	M	18	16		19	10		19	15		18	14		15	18	
	L	21	12		21	14		17	22		19	23		15	22	
I.5 Web-browsers/systems/ applications to remember password	H	60	62	0.82436	56	76	**0.00022***	60	**62**	0.11921	59	69	0.22469	64	59	0.43884
	M	18	16		19	13		21	14		19	14		18	18	
	L	21	22		25	11		20	24		22	17		18	23	
I.6 Locking workstation when away from desk	H	29	37	0.27171	26	**47	**2.23E-05***	29	33	0.25851	30	35	0.70499	30	31	0.99639
	M	25	27		27	22		24	27		26	24		26	25	
	L	45	37		48	31		47	40		44	42		44	44	
I.7 Using a password to log in home computer	H	20	36	**0.00068***	19	35	**0.00010***	20	26	0.24451	22	29	0.16294	24	22	0.54872
	M	11	17		11	15		14	11		12	15		14	12	
	L	69	48		70	50		66	64		67	56		62	67	
I.8 Logging off from online systems before closing the browser/app	H	54	69	**0.00216***	51	73	**7.97E-05***	55	57	0.10653	55	64	0.23981	63	53	**0.03605***
	M	21	17		22	14		18	23		21	18		17	22	
	L	25	14		27	13		27	20		25	18		20	25	

II. Social Networks Behaviors	Risk Level	Percentage (%)														
		Sample	IT proficiency			Age (in years)				Gender			Online Activity			
			IT pro	Non-IT pro	p-value	18-30	31-50	51+	p-value	Male	Female	p-value	High	Medium	Low	p-value
II.1 Engaging in social networks	H	86	87	86		91	82	59		84	92		72	92	72	
	M	9	6	10	0.11081	6	13	15	0.10037	9	7	0.72948	17	6	17	0.68835
	L	5	6	4		3	5	26		7	1		11	2	11	
II.2 Accepting invitations from unknown persons	H	21	15	27		23	20	11		23	18		23	22	19	
	M	21	20	22	0.39483	23	20	14	0.25046	21	21	0.38701	21	23	20	0.66158
	L	58	65	50		54	61	74		56	62		56	55	61	

II. Social Networks Behaviors	Risk Level	Percentage (%)													
		Openness			Conscientiousness			Extraversion			Agreeableness			Neuroticism	
		BFI+	BFI-	p-value	BFI+	BFI-	p-value	BFI+	BFI-	p-value	BFI+	BFI-	p-value	BFI+	BFI-	p-value
II.1 Engaging in social networks	H	86	87		85	90		89	**83**		87	82		90	85	
	M	9	8	0.93323	9	6	0.39412	7	11	0.13765	8	11	0.43778	6	10	0.25230
	L	5	6		5	5		4	6		5	7		4	5	
II.2 Accepting invitations from unknown persons	H	20	28		18	33		21	22		19	32		28	18	
	M	23	14	0.11106	20	26	0.48305	22	20	0.87055	22	18	0.07209	18	23	0.40162
	L	57	58		62	41		57	58		59	50		54	59	

III. Security Software Behaviors	Risk Level	Percentage (%)														
		Sample	IT proficiency			Age (in years)				Gender			Online Activity			
			IT pro	Non-IT pro	p-value	18-30	31-50	51+	p-value	Male	Female	p-value	High	Medium	Low	p-value
III.1 Updating AntiVirus software	H	30	14	**44	**4.09E-14***	31	30	7	**0.03017***	27	37	**0.03924***	19	31	37	**0.00058***
	M	18	18	17		19	15	22		18	18		15	20	19	
	L	52	68	39		50	55	70		55	45		66	49	45	
III.2. Installing latest security patches	H	41	23	52	**2.35E-11***	41	36	33	0.726303	32	55	**2.73E-06***	24	42	47	**1.30E-07***
	M	24	33	21		26	27	26		29	21		23	32	24	
	L	35	**44	27		33	**38	**41		**40	24		**53	26	29	
III.3. Disabling Antvirus/Firewall	H	24	13	31	**1.50E-06***	24	21	15	**0.02862***	22	24	0.76822	17	24	26	0.33791
	M	17	19	19		21	15	19		19	17		22	19	17	
	L	59	68	50		55	64	67		59	58		61	57	57	
III.4.Canceling or postponing security updates	H	43	31	55	0.13107	47	39	37	0.28574	39	55	0.24975	34	51	45	0.45205
	M	29	37	22		30	25	33		31	24		25	33	29	
	L	28	**33	23		23	36	30		30	21		**41	17	26	
III.5.Installing/using pirate software	H	42	45	40	0.34286	51	29	15	**2.625E-10***	48	28	**0.00011***	53	42	34	**0.00223***
	M	21	21	21		22	21	7		19	25		22	19	22	
	L	37	34	40		27	**50	**78		33	47		25	39	**44	

III. Security Software Behaviors	Risk Level	Percentage (%)														
		Openness			Conscientiousness			Extraversion			Agreeableness			Neuroticism		
		BFI+	BFI-	p-value	BFI+	BFI-	p-value	BFI+	BFI-	p-value	BFI+	BFI-	p-value	BFI+	BFI-	p-value
III.1. Updating AntiVirus software	H	28	40	**0.03048***	25	**46	**1.658-06***	29	31	0.67995	28	40	0.07110	35	27	**0.03958***
	M	18	17		17	20		19	16		19	11		18	18	
	L	54	43		58	33		52	53		53	49		46	56	
III.2. Installing latest security patches	H	36	51	**0.00242***	34	54	**0.00013**	38	40	0.51867	37	46	**0.03572**	48	34	**0.00291**
	M	27	23		28	22		28	24		26	31		26	27	
	L	**37	26		**38	23		34	36		37	23		27	**39	
III.3. Disabling Antvirus/Firewall	H	20	36	**0.00570***	18	38	**3.68E-06***	20	26	0.24671	21	33	**0.00298***	26	21	0.13993
	M	20	14		19	19		20	18		19	19		21	18	
	L	60	50		63	42		60	56		61	48		52	62	
III.4.Canceling or postponing security updates	H	40	61	0.06149	37	66	0.37708	45	42	0.77864	42	55	0.07515	53	39	0.67244
	M	31	16		32	17		29	29		32	21		22	32	
	L	28	23		31	17		26	29		28	24		25	29	
III.5.Installing/using pirate software	H	41	50	0.21415	38	56	**0.00106***	44	41	0.38478	39	58	**0.00546***	45	41	0.23510
	M	22	16		21	19		19	24		22	14		23	19	
	L	37	34		**40	25		38	36		39	27		32	39	

IV. Email Security Behaviors	Risk Level	Percentage (%)														
		Sample	IT proficiency			Age (in years)				Gender			Service Usage			
			IT pro	Non-IT pro	p-value	18-30	31-50	51+	p-value	Male	Female	p-value	High	Medium	Low	p-value
IV.1. Clicking on links/Attachments within emails from unknown sources	H	15	8	22	**7.52E-06***	15	16	7	0.457885	13	22	**0.00227***	15	14	17	0.00481*
	M	22	21	22		20	24	30		21	22		20	19	25	
	L	63	71	56		65	60	63		66	57		66	67	58	
IV.2.Clicking on links/Attachments within emails from friends without checking	H	44	31	55	**2.15E-08***	44	45	37	0.379267	41	51	**0.00132***	37	47	46	**0.03146***
	M	28	30	26		26	30	41		27	29		25	28	31	
	L	28	**39	19		31	25	22		32	20		**38	26	23	
IV.3. Deleting suspicious emails	H	25	22	28	**0.00615***	32	18	0	**0.00257***	26	22	0.33558	22	24	29	0.16202
	M	19	21	17		18	20	19		20	17		16	24	17	
	L	56	57	55		51	62	81		54	61		62	52	54	
IV.4. Notifying IT support when receiving suspicious emails	H	72	80	65	0.79935	81	57	59	**1.201E-08***	75	65	0.06929	70	71	75	0.54360
	M	14	11	16		11	20	7		12	18		13	15	13	
	L	14	10	19		8	23	33		13	17		18	14	12	
IV.5.Forwarding chain emails	H	12	4	20	**4.54E-09***	12	14	0	0.239735	12	12	0.75911	10	12	14	**0.00279***
	M	10	8	12		9	11	15		9	12		6	11	12	
	L	78	88	68		79	75	85		78	76		84	78	73	

IV. Email Security Behaviors	Risk Level	Percentage (%)														
		Openness			Conscientiousness			Extraversion			Agreeableness			Neuroticism		
		BFI+	BFI-	p-value	BFI+	BFI-	p-value	BFI+	BFI-	p-value	BFI+	BFI-	p-value	BFI+	BFI-	p-value
IV.1. Clicking on links/Attachments within emails from unknown sources	H	13	26	**0.00813***	12	26	**0.00063***	15	16	0.91656	13	26	**0.03860***	18	14	0.22025
	M	21	22		21	22		22	21		22	17		23	21	
	L	65	52		67	52		64	63		64	57		59	66	
IV.2.Clicking on links/Attachments within emails from friends without checking	H	42	54	0.07244	40	56	**0.00239***	43	45	0.56589	41	56	0.01152	47	42	0.46392
	M	29	21		31	18		30	26		30	15		26	29	
	L	29	24		29	26		27	30		28	29		27	29	
IV.3. Deleting suspicious emails	H	24	33	**0.04942***	23	31	**0.04850***	24	27	0.45458	24	35	**0.03283***	29	23	0.38490
	M	18	22		18	22		20	17		19	19		18	19	
	L	58	44		59	46		56	56		58	46		52	58	
IV.4. Notifying IT support when receiving suspicious emails	H	71	77	0.57094	71	77	0.22078	70	74	0.50080	72	74	0.78652	75	71	0.54910
	M	14	11		14	14		15	12		13	14		13	14	
	L	15	12		16	10		15	14		15	12		13	15	
IV.5.Forwarding chain emails	H	11	20	**0.00905***	9	22	**0.00019***	14	11	0.48219	9	27	**2.38E-05***	16	10	0.16138
	M	9	14		9	14		9	11		10	10		11	10	
	L	80	66		82	65		77	79		80	63		73	80	

V. Data Management Behaviors	Risk Level	Percentage (%)														
		Sample	IT proficiency			Age (in years)				Gender			Online Activity			
			IT pro	Non-IT pro	p-value	18-30	31-50	51+	p-value	Male	Female	p-value	High	Medium	Low	p-value
V.1. Backing up data on a regular basis	H	48	48	47	0.00934*	56	34	33	**8.97E-05***	51	39	0.07745	41	51	51	**0.00104***
	M	25	24	26		20	33	30		21	33		20	26	28	
	L	27	27	27		24	33	**37		27	28		40	24	21	
V.2. Using an encrypted USB drive to transfer files between computers	H	83	89	77	0.07525	84	82	74	0.17723	84	79	0.33660	78	86	83	0.22137
	M	10	8	14		12	10	11		10	13		12	11	10	
	L	7	3	9		5	9	15		6	8		10	3	7	
V.3. Scanning a USB drive before using it	H	68	66	69	0.52662	69	66	59	0.05810	64	76	**0.001638***	56	76	70	**0.00045***
	M	17	19	15		18	17	7		18	16		20	12	19	
	L	15	15	15		13	17	33		18	8		24	12	11	
V.4. Inserting and accessing USB/CD/DVD from unknown sources	H	30	19	**41	**1.57E-07***	29	34	22	0.14022	30	32	0.71547	30	29	32	0.87682
	M	30	35	26		33	28	19		30	31		30	29	32	
	L	40	46	33		38	38	59		40	37		39	42	37	
V.5. Encrypting sensitive information on the device	H	74	71	77	**0.00257***	76	71	81	0.36144	71	83	**0.00181***	64	79	79	**0.04969***
	M	14	17	12		14	17	4		16	10		20	13	11	
	L	12	12	10		11	12	15		13	8		16	8	10	
V.6. Destroying all data before disposal of hardware	H	34	25	42	**0.00024***	37	30	22	**0.00881***	31	42	**0.04889***	22	37	40	**0.00215***
	M	19	21	17		20	18	11		20	17		19	21	17	
	L	47	54	41		43	52	67		50	42		59	42	43	
V.7. Opening a document despite security warnings	H	51	54	47	0.06612	58	39	30	**1.071E-08***	51	49	0.87821	54	54	44	**0.00191***
	M	32	33	32		31	36	22		32	33		31	34	32	
	L	17	13	21		11	26	**48		17	19		15	12	24	
V.8. Downloading files from suspicious websites	H	31	27	35	0.73422	**35	28	15	**0.00058***	32	31	0.18625	32	31	31	0.36998
	M	32	39	27		35	29	19		34	28		30	**38	30	
	L	37	34	38		30	43	67		34	42		37	31	40	

V. Data Management Behaviors	Risk Level	Percentage (%)														
		Openness			Conscientiousness			Extraversion			Agreeableness			Neuroticism		
		BFI+	BFI-	p-value	BFI+	BFI-	p-value	BFI+	BFI-	p-value	BFI+	BFI-	p-value	BFI+	BFI-	p-value
V.1. Backing up data on a regular basis	H	47	52	0.13872	41	70	**3.51E-08***	45	51	0.20385	46	56	0.22717	54	44	0.06579
	M	24	29		27	17		24	26		26	19		20	27	
	L	29	19		32	13		30	24		28	25		26	28	
V.2. Using an encrypted USB drive to transfer files between computers	H	82	85	0.86497	81	86	0.42297	80	85	0.29207	81	89	0.19223	83	82	0.88717
	M	11	10		12	9		12	10		12	6		10	11	
	L	7	6		7	5		8	5		7	5		7	6	
V.3. Scanning a USB drive before using it	H	65	80	**0.00227***	64	80	**0.00281***	67	69	0.28290	67	71	0.71763	73	65	**0.00945***
	M	18	11		19	12		16	18		17	15		18	17	
	L	17	9		17	8		17	13		16	13		9	19	
V.4. Inserting and accessing USB/CD/DVD from unknown sources	H	30	34	0.66809	27	**42	**0.00636***	33	28	0.07707	29	**40	0.08393	33	29	0.39209
	M	31	29		31	28		26	35		31	24		32	30	
	L	40	37		42	30		41	37		40	36		35	41	
V.5. Encrypting sensitive information on the device	H	73	81	0.26621	73	80	0.18712	71	79	0.05438	74	75	0.44059	80	72	0.15971
	M	15	11		16	10		17	11		13	20		11	16	
	L	12	8		12	10		12	11		13	5		9	12	
V.6. Destroying all data before disposal of hardware	H	31	**48	**0.00218***	31	**43	**0.00270***	35	32	0.47316	32	**45	**0.00373***	39	31	**0.04103***
	M	19	21		18	23		17	21		19	20		20	19	
	L	50	31		51	33		48	46		50	35		41	50	
V.7. Opening a document despite security warnings	H	48	59	0.15292	45	66	**6.84E-05***	50	51	0.90317	46	70	**0.00033***	53	49	0.31344
	M	34	24		34	26		33	32		35	19		33	32	
	L	18	17		20	8		18	17		19	11		14	19	
V.8. Downloading files from suspicious websites	H	30	**39	0.23786	27	**46	**4.36E-05***	31	32	0.32491	29	**46	**0.00082***	**36	29	**0.00191***
	M	33	28		32	32		30	35		32	33		35	31	
	L	37	33		41	22		39	33		39	20		28	40	

VI. Network Management Behaviors	Risk Level	Percentage (%)														
		Sample	IT proficiency			Age (in years)				Gender			Service Usage			
			IT pro	Non-IT pro	p-value	18-30	31-50	51+	p-value	Male	Female	p-value	High	Medium	Low	p-value
VI.1 Disabling wireless technologies when not using it	H	62	67	66	0.06211	61	62	74	0.62739	58	71	**0.00688***	57	63	65	0.63775
	M	19	23	16		19	21	15		20	19		22	19	18	
	L	19	21	17		20	17	11		22	11		22	19	17	
VI.2 Connecting to public access WiFi networks	H	70	60	80	**0.03617***	73	68	52	**0.04305***	68	78	0.41972	77	72	64	**0.00274***
	M	22	31	13		20	24	22		16	15		17	21	25	
	L	8	10	7		7	7	26		22	8		6	7	10	
VI.3 Using the TOR network	H	63	64	65	0.06274	62	65	85	**0.42750***	59	75	**0.00492***	64	61	67	0.08255
	M	17	17	18		17	21	0		19	12		14	16	20	
	L	18	19	17		21	14	15		22	13		22	23	13	
VI.4 Using an anonymizing proxy	H	48	48	45	0.09375	44	52	81	**0.00379***	41	65	**0.00286***	42	48	54	**0.00283***
	M	21	21	25		22	21	7		22	19		20	20	24	
	L	30	31	30		34	27	12		37	16		40	32	22	
VI.5 Using a VPN	H	82	83	84	0.48229	86	76	85	0.07351	81	85	0.58261	75	85	86	**0.00592***
	M	13	13	14		10	20	11		13	13		17	11	12	
	L	4	4	2		4	4	4		6	2		8	4	2	

VI. Network Management Behaviors	Risk Level	Percentage (%)														
		Openness			Conscientiousness			Extraversion			Agreeableness			Neuroticism		
		BFI+	BFI-	p-value	BFI+	BFI-	p-value	BFI+	BFI-	p-value	BFI+	BFI-	p-value	BFI+	BFI-	p-value
VI.1 Disabling wireless technologies when not using it	H	60	71	0.13646	60	70	**0.04583***	63	61	0.80543	62	62	0.79378	60	63	0.82981
	M	20	16		20	16		18	21		19	21		21	19	
	L	20	13		20	14		19	18		19	17		19	19	
VI.2 Connecting to public access WiFi networks	H	69	76	0.50767	70	73	0.80246	72	69	0.28085	70	76	0.43556	73	69	0.67052
	M	22	18		22	20		22	21		22	17		20	22	
	L	8	7		8	7		6	10		8	7		7	8	
VI.3 Using the TOR network	H	64	62	0.08264	65	60	0.06264	68	59	0.07749	65	57	**0.02649***	63	65	0.07329
	M	17	19		17	18		14	21		18	13		17	17	
	L	19	19		18	22		18	20		17	30		20	18	
VI.4 Using an anonymizing proxy	H	49	47	0.41756	51	39	**0.00517***	52	44	0.33049	49	43	0.25406	46	49	0.29446
	M	21	20		22	18		20	23		22	18		21	21	
	L	30	33		27	42		28	33		29	30		33	30	
VI.5 Using a VPN	H	81	91	**0.04467***	82	85	0.19953	83	82	0.38145	83	79	0.58315	80	84	0.23196
	M	14	8		14	11		13	13		12	18		15	12	
	L	5	1		4	4		4	5		5	3		5	4	

Appendix C : A List of Users' Behaviors in the Context of Mobile Devices and How To Monitor Them

When looking at mobile device usage, these behaviors could usefully be classified as:

I. System/Device related behaviors					
No.	**Process**	**User behavior**			**How to Monitor**
1	Location services: Access to my location	On			The method `IsProviderEnabled` of the class `LocationManager` provides access to the system location services. If the user has enabled this provider (`GPS_PROVIDER, NETWORK_PROVIDER`) in the Settings menu, true is returned otherwise false is returned. Another option is by using The Google Location Services API, part of Google Play Services, which provides a powerful, high-level framework that automatically handles location providers, user movement, and location accuracy
		Off			
2	Google location history: Allows Google to regularly obtain location data	On			
		Off			
3	Screen lock	Select Face/pattern/pin or password			Use `KeyguardManager` to determine the state and security level of the keyguard. `KeyGuardManager.isDeviceSecure()` returns true if the device is secured with a PIN, pattern or password.
		None			
4	Automatically lock	Either immediately			The `Settings.System` provider offers a `SCREEN_OFF_TIMEOUT` setting that specifies the amount of time in milliseconds before the device goes to sleep or begins to dream after a period of inactivity. This value is also known as the user activity timeout period since the screen isn't necessarily turned off when it expires
		or after 30 seconds			
		1min/2min …etc			
		the longer the time period the more the risk			
5	Make passwords visible (during entry)	On			`Settings.System.TEXT_SHOW_PASSWORD` is to show password characters in text editors. 1 = On, 0 = Off
		Off			
6	Unknown sources: to allow the installation of non-market apps	On.	The system notifies the user of the consequences.	Select OK	The `INSTALL_NON_MARKET_APPS` Of `Settings.Secure` returns whether applications can be installed for this user via the

I. System/Device related behaviors				
No.	**Process**		**User behavior**	**How to Monitor**
			Select Cancel	system's `ACTION_INSTALL_PACKAGE` mechanism. Android keeps track of how a package was installed through the method `getInstallerPackageName` that identifies which market the package (app) came from.
			Off	
7	Owner Info: Text that appears on the lock screen		Entering name, date of birth, address, phone number, email or a hello message	`LOCK_SCREEN_OWNER_INFO`.This preference contains the string that shows for owner info on LockScreen. OR use the `getDeviceOwnerLockScreenInfo` method of the `DevicePolicyManager` class. It returns the device owner information. If it is not set returns null.
8	Privacy protection: To set two modes (passwords) one for guest and the other for owner of device		Activation of this feature	To get the number of user profiles use `UserManager.getUserCount()`. To identify which user profile is activated, `UserManager um = (UserManager) getContext().getSystemService(Context.USER_SERVICE); um.isSystemUser();` With that it can be identified if the user is different of the system user. Whereas `getAccounts()` of the `AccountManager` class Lists all accounts of any type registered on the device.
			Unlock with guest password, then all private information will be hidden	
			Unlock with owner password	
9	Device administrators	Suspend button (to allow the app suspend button to erase all data, change the screen	Activate	The method `getPackageName()` of the class `DeviceAdminInfo` Return the .apk package that implements this device admin.

<table>
<tr><th colspan="8">I. System/Device related behaviors</th></tr>
<tr><th>No.</th><th colspan="3">Process</th><th colspan="3">User behavior</th><th>How to Monitor</th></tr>
<tr><td></td><td colspan="2"></td><td>unlock password, set password rules, monitor screen unlock attempts and lock the screen)</td><td colspan="3">Deactivate</td><td></td></tr>
<tr><td></td><td colspan="2"></td><td rowspan="2">Android device manager
(to allow the app Google Play services to erase all data, change the screen unlock password, and lock the screen)</td><td colspan="3">Activate</td><td></td></tr>
<tr><td></td><td colspan="2"></td><td colspan="3">Deactivate</td><td></td></tr>
<tr><td rowspan="2">10</td><td colspan="3" rowspan="2">Backup and restore</td><td rowspan="2">Off.</td><td rowspan="2">When selected, the system notifies the user of the consequences.</td><td>Select OK</td><td rowspan="3">By checking that the Backup Manager is operational using the bmgr enabled command: <code>adb shell bmgr enabled</code></td></tr>
<tr><td>Select Cancel</td></tr>
<tr><td colspan="3">On</td><td></td></tr>
<tr><td>11</td><td colspan="3">Automatic restore: when an app is reinstalled, all backed up settings and data are restored</td><td colspan="3">On</td><td></td></tr>
<tr><td></td><td colspan="3"></td><td colspan="3">Off</td><td></td></tr>
<tr><td>12</td><td colspan="3">Factory data reset</td><td colspan="3">Reset phone. This is a good practice before disposal of device</td><td>TBC</td></tr>
<tr><td rowspan="2">13</td><td rowspan="2">Google account</td><td colspan="2" rowspan="2">Ads: Instruct apps not to use user’s advertising ID to build profiles or personalized apps</td><td colspan="3">On.</td><td rowspan="2">TBC</td></tr>
<tr><td colspan="3">Off.</td></tr>
<tr><td rowspan="2">14</td><td rowspan="2">Updater</td><td rowspan="2">Update settings</td><td rowspan="2">Auto check for updates</td><td rowspan="2">Off</td><td rowspan="2">The system will notify the user that it will not check for updates.</td><td>Cancel</td><td rowspan="2">TBC</td></tr>
<tr><td>Off</td></tr>
</table>

I. System/Device related behaviors					
No.	**Process**			**User behavior**	**How to Monitor**
				On	
			Auto download via Wi-Fi	On	
				Off	
			Check for system updates	To check for available system updates	
15	Wi-Fi			On	The method `isWifiEnabled()` of the class `WifiManager` returns whether Wi-Fi is enabled or disabled. The `getNetworkId ()` method of the `WifiInfo` class returns the ID for the currently connected network or -1 if no network is connected. `WIFI_NETWORKS_AVAILABLE_NOTIFICATION_ON` of the class `Settings.Global` determines whether to notify the user of open networks.
				Off	
		Settings	Network notification to notify the user when an open network is available	On	
				Off	
16	Bluetooth			On	The method `isEnabled()` of the class `BlueToothAdapter` Returns true if Bluetooth is currently enabled and ready for use. Or by using `BLUETOOTH_ON` of the class `Settings.Global` that specifies whether bluetooth is enabled/disabled
				Off	
		Visibility to all bluetooth devices nearby		On	The method `getScanMode()` of the class `BluetoothAdapter g`ets the current Bluetooth scan mode of the local Bluetooth adapter. It determines if the local adapter is connectable and/or discoverable from remote Bluetooth devices. Or by using the `BLUETOOTH_DISCOVERABILITY` of
				Off	

I. System/Device related behaviors					
No.	**Process**		**User behavior**		**How to Monitor**
					the class `Settings.System` that determines whether remote devices may discover and/or connect to this device
17	Accounts: Google	Safe search filter	On		TBC
			Off		
		Block Pornography and offensive content	On		
			Off		
18	Mobile hotspot	Portable Wi-Fi hotspot	On		This could be detected programmatically by the use of the `WifiApManager` class and the method `isWifiApEnabled()as in http://stackoverflow.com/questions/11841421/how-to-get-wifi-hotspot-state`
			Off		
		Settings	Add device		The list of devices connected can be obtained programmatically as in http://stackoverflow.com/questions/29249441/how-to-listen-devices-connected-to-android-hotspot
			Allow all devices to connect automatically	On	
				Off	
19	NFC: allow data exchange when the phone touches another device		On		Using `NfcAdapter.getDefaultAdapter()` to get the adapter (if available) and call its `isEnabled()` method to check whether NFC is currently turned on.
			Off		
20	Camera settings	GPS tag to attach location information to each video or photo taken	Enable		There's no way to confirm if that setting is enabled or not, since it's not part of any public or standard Android API. But by the use of permissions, the accessibility API `AccessabilityService` could be used to read these settings.
			Disable		
21	Google Play settings	Auto update apps	Do not		TBC
			auto update at any time		
			over Wi-Fi only		
		Notify me when an App update is available	On		
			Off		

I. System/Device related behaviors				
No.	**Process**		**User behavior**	**How to Monitor**
		Notify me when Apps are automatically updated	On	
			Off	
		Require authentication for purchases on Google Play	On	
			Off	

For example, The Android SDK has several classes for settings such as:

- Class Settings.Secure
  Secure system settings, containing system preferences that applications can read but are not allowed to write. These are for preferences that the user must explicitly modify through the system UI or specialized APIs for those values, not modified directly by applications.
- Class Settings.Global
  Global system settings, containing preferences that always apply identically to all defined users. Applications can read these but are not allowed to write; like the "Secure" settings, these are for preferences that the user must explicitly modify through the system UI or specialized APIs for those values.
- Class Settings.System
  System settings, containing miscellaneous system preferences. This table holds simple name/value pairs. There are convenience functions for accessing individual settings entries.

A list of all installed apps could be obtained programmatically by the use of the method `getInstalledApplications` of the `packageManager`. The method `getInstallerPackageName` gets the name of the package that installed the application.

To check if installed apps are all updated (latest versions), the `packageInfo` class and `versionCode` returns the version number of this package, `lastUpdateTime` gives The time at which the app was last updated. Or use this Android Library: https://github.com/danielemaddaluno/Android-Update-Checker.

<table>
<tr><th colspan="7">II. Application-related behaviors</th></tr>
<tr><th>Category</th><th>App</th><th>No.</th><th colspan="3">Process</th><th>User behavior</th><th>How to monitor</th></tr>
<tr><td rowspan="8">Social Networks</td><td rowspan="8">Twitter</td><td>1</td><td colspan="3">Sign in</td><td>Enter user name and password. Password could be weak, old or reused</td><td>A separate password table could be created for all app accounts. These passwords will be hashed and salted. Upon entry of password, various password defined- rules set could be checked using vt-password (passay) library which is a password policy enforcement for JAVA. For example, <code>HistoryRule</code> is a rule for determining if a password matches one of any previous password a user has chosen. If no historical password reference has been set, then passwords will meet this rule.
One or more password rule is violated
All password rules are met</td></tr>
<tr><td>2</td><td colspan="3">Open tweets</td><td>Read/browse tweets timeline</td><td rowspan="2">Traffic analysis</td></tr>
<tr><td>3</td><td colspan="3">Refresh home</td><td>Refresh home page</td></tr>
<tr><td>4</td><td colspan="3">Browse contacts</td><td>Read contacts whether following or followers</td><td>The <code>GET friends/ids</code> request returns a collection of user IDs for every user the specified user is following.
The <code>GET followers/ids</code> request Returns a collection of user IDs for every user following the specified user.</td></tr>
<tr><td>5</td><td colspan="3">Browse notifications</td><td>Read notifications</td><td rowspan="3">By using Twitter APIs, Twitter allows to interact with its data ie tweets & several attributes about tweets.
This field could be determined by the request <code>GET account/settings.</code></td></tr>
<tr><td rowspan="2">6</td><td>Noti-fications</td><td>settin gs</td><td>only people you follow</td><td>On</td></tr>
<tr><td colspan="3">Off</td></tr>
<tr><td>7</td><td colspan="3">Message/ Tweet/</td><td>Send direct messages to followers</td><td>Message content could be text, photos/videos, GIF, URL and/or location.</td></tr>
</table>

II. Application-related behaviors					
Category	**App**	**No.**	**Process**	**User behavior**	**How to monitor**
			Retweet		Text message: depending on content of message. For example, could be offensive comments about disabilities, age, religious beliefs and sexual orientation Photos/videos: personal photo or video of children, credit card, military base …etc from camera photo album that may include additional hidden info such as location Location: send current location. Message content will be monitored to identify any disruptive, offensive message or personal information such as passwords or credit card numbers. A list of predefined black words or phrases could be created, then by the implementation of a keystroke logger and text analysis the message content will be scanned against that list such that if any undesirable/risky content is detected it is picked up and flagged. For multimedia content: facial detection and recognition techniques could be applied to determine persons in the file that might give rise to privacy related issues and user notified. To differentiate between photos and videos, the mimeType is used to check if the file path corresponds to an image or video. Location: check for GPS coordinates location data embedded in a photo. This information could be obtained by using an EXIF (Exchange Image File Format) viewer. URL: phishing detection engines will be used to check for its legitimacy Social networks analysis techniques could be used to determine relationships between social entities.

II. Application-related behaviors					
Category	**App**	**No.**	**Process**	**User behavior**	**How to monitor**
					Further to that, attributes such as recipients, degree of relationship in the social network (if any) and type of account may escalate the risk level of this process.
				Publish a message or tweet.	Message content is safe
				Retweet a message.	Message has disruptive/offensive content
		8	Reply	Same as in process of "Tweet/ Message/ Retweet" except that the sender is in the follower/following list and reply is to a single message	Message has privacy related issues such as bank account number or the user's child photo
		9	Edit profile	Adding personal information such as location, birthday and phone number. Could be used in identity theft or for guessing user's passwords	The `url` filed of `Users` object returns the URL provided by the user in association with their profile. So as `name` and `location` fields return the name of the user, as they've defined it and the user-defined location for this account's profile respectively.
		10	Like tweet	Low risk. But content liked may escalate the risk level.	TBC
		11	login verification (To add additional verification to protect account. This could be used as a metric for IT expertise)	On	TBC
				Off	
		12	Protect my tweets	On: private account	This could be returned by the `GET account/settings` request . The `protected` field of `Users` object, When true, indicates that this user has chosen to protect their
				Off: public account	

II. Application-related behaviors						
Category	**App**	**No.**	**Process**	**User behavior**	**How to monitor**	
					Tweets.	
		13	Receive direct messages from anyone	On	**The account settings object has an *allow_dms_from* field which indicates who can DM (direct message) a user, either in a private one-on-one thread or in a group thread.**	Possible values include “following”
						Or “all”
				Off		
		14	Photo tagging	On	This could be returned by the `GET account/settings` request . The field `geo_enabled` of `Users` object, When true, indicates that the user has enabled the possibility of geotagging their Tweets	Protected
						Public
				Off		
		15	Let others find me by email address/ phone number	On	This could be returned by the `GET account/settings` request. If the field `discoverable_by_email` is true, then it is on	
				Off		
	Facebook	1	Read news feed	Browsing latest posts from friends, suggested posts and pages you follow	The Facebook SDK for Android is used to integrate an app with Facebook and enquire about its data thru APIs. The Graph API is the primary way to get data in and out of Facebook's social graph. The Android SDK has support for integrating with Facebook Graph API. With the `GraphRequest` and `GraphResponse` classes, one could make requests and get responses in JSON asynchronously. Moreover, batch requests could be made with a single round-trip to the Facebook servers with `GraphRequestBatch`.	

II. Application-related behaviors						
Category	**App**	**No.**	**Process**		**User behavior**	**How to monitor**
						The **`/{user-id}/feed`** Returns the feed of posts (including status updates) and links published by this person, or by others on this person's profile. There are other edges which provide filtered versions of this edge: `/{user-id}/posts` shows only the posts that were published by this person. `/{user-id}/tagged` shows only the posts that this person was tagged in.
		2	Friend requests:	from someone I know	Confirm request.	A user represents a person on Facebook. The `/{user-id}` node returns a single user and `/{user-id}/accounts` returns Facebook Pages this person administers/is an admin for
					Decline request.	
				through a mutual friend	Confirm request.	Use social network analysis to determine relationship degree with this mutual friend and notify user of it. The `/{user-id}/friendlists` reads a user's friend list on Facebook While `all mutual friends` Returns a list of all the Facebook friends that the session user and the request user have in common
					Decline request.	
		3	Add friend		Request a connection with People I may know	TBC
					Request a connection through a mutual friend	TBC
		4	Remove friend		Remove the friend request	TBC
		5	Read user profile		Read the user profile if public	TBC
					Read only mutual friends if private	TBC
		6	Read notifications		Read notifications from friends	TBC
		7	Login alerts		ON. To be alerted (email/Facebook	When logging in to Facebook, the site looks up the

II. Application-related behaviors					
Category	**App**	**No.**	**Process**	**User behavior**	**How to monitor**
				notification) when someone logs into my account from an unrecognized device	last location you logged in from (by geolocating the IP address), and compares it to a list of 'known' locations. If the location the user is logging in from is beyond a certain 'distance threshold' from the known locations, or not
				Off	
		8	Third party authenticator	Set up a third party app to generate Facebook security codes for login approvals/reset password. Med risk	TBC
		9	Generate app password	Type the name of the app	TBC
		10	Recognized devices/ where you logged in	Approve	TBC
				Delete	
		11	Who can see my stuff	Select audience who can see future posts/ see people and lists you follow	The Graph API does not provide any means to access the user's privacy settings. However, the user object (see http://developers.facebook.com/docs/reference/api/user/) allows you to access all the privacy-related information, but does not let you access the user's privacy settings. One way to get around this is by pulling the privacy settings of objects they've posted previously and see what the most common setting is, and then guess from that what their defaults are. For processes 11-14, the options are: Public (everyone)
		12	Who can contact me	Who can send friend request either everyone or friends of friends	friends
		13	Who can look you up	Using provided email or using provided phone number/ search engines.	Friends of friends
		14	Timeline and tagging	Who can add things to my timeline.	Only me
				Who can see things on my timeline	
				Who can follow me either public or friends	

II. Application-related behaviors					
Category	**App**	**No.**	**Process**	**User behavior**	**How to monitor**
		15	Post on wall	Text	`/{user-id}/photos` reads Photos the person is tagged in or has uploaded. While `/{user-id}/picture` gets the person's profile picture. Message content could be text, photos/videos, GIF, URL and/or location. Text message: depending on content of message. For example, could be offensive comments about disabilities, age, religious beliefs and sexual orientation Photos/videos: personal photo or video of children, credit card, military base …etc from camera photo album that may include additional hidden info such as location Location: send current location Message content will be monitored to identify any disruptive, offensive message or personal information such as passwords or credit card numbers. A list of predefined black words or phrases could be created, then by the implementation of a keystroke logger and text analysis the message content will be scanned against that list such that if any undesirable/risky content is detected it is picked up and flagged. For multimedia content: facial detection and recognition techniques could be applied to determine persons in the file that might give rise to privacy related issues and user notified. To differentiate between photos and videos, the `mimeType` is used to check if the file path corresponds to an image or video Location: check for GPS coordinates location data embedded in a photo. This information could be obtained by using an EXIF (Exchange Image File
				Photos/videos	
				Check in: expose current location	

II. Application-related behaviors						
Category	**App**	**No.**	**Process**	**User behavior**		**How to monitor**
						Format) viewer. URL: phishing detection engines will be used to check for its legitimacy. Social networks analysis techniques could be used to determine relationships between social entities. However, the user will be notified of consequences if this post is shared publically.
				Add activity		TBC
				Share post with	Public	Message content is safe
						Message has offensive/disruptive content
						Message has privacy related issues such as bank account number or photo of user's chil
					Friends, friends except, close friends	Message content is safe
						Message has offensive/disruptive content
						Message has privacy related issues such as bank account number or photo of user's chil
					Only me	Message content is safe
						Message has offensive/disruptive content
						Message has privacy related issues such as bank account number or photo of user's chil
		16	Like/love/wow/sad…etc.	Select one of them		`/{user-id}/likes` reads all pages this user liked
		17	Comment	Write a comment.	Public account	Comment text will be monitored and scanned to identify any disruptive, offensive message or personal information and user will be alerted.
						Message content is safe
						Message has offensive/disruptive content
						Message has privacy related issues such as bank account number or photo of user's child
					Private account	Message content is safe
						Message has offensive/disruptive content
						Message has privacy related issues such as bank

II. Application-related behaviors					
Category	**App**	**No.**	**Process**	**User behavior**	**How to monitor**
					account number or photo of user's child
		18	Share	Share post.	Traffic analysis. User is alerted for consequences of sharing sensitive, disruptive or personal information with others.
		19	Search Facebook	Search for profiles on Facebook	TBC
		20	Tag friends	Select whom to tag	TBC
		21	Update profile	Add personal information such as Birthdate, phone number, hobbies, favorite books, location …etc.	The Graph API call `https://graph.facebook.com/bgolub?fields=id,name,picture` will only return the id, name, and picture in the defined profile. If null, then nothing was added.
Messaging	**WhatsApp**	1	Send /forward/ reply message		Message content could be text, photos/videos, GIF, URL and/or location. Text message: depending on content of message. For example, could be offensive comments about disabilities, age, religious beliefs and sexual orientation Photos/videos: personal photo or video of children, credit card, military base …etc from camera photo album that may include additional hidden info such as location Location: send current location. Message content will be monitored to identify any disruptive, offensive message or personal information such as passwords or credit card numbers. A list of predefined black words or phrases could be created, then by the implementation of a keystroke logger and text analysis the message content will be scanned against that list such that if any undesirable/risky content is detected it is picked up and flagged. For multimedia content: facial recognition techniques could be applied to determine persons in the file that might give rise to privacy related

II. Application-related behaviors						
Category	**App**	**No.**	**Process**	**User behavior**		**How to monitor**
						issues and user notified. To differentiate between photos and videos, the mimeType is used to check if the file path corresponds to an image or video Location: check for GPS coordinates location data embedded in a photo. This information could be obtained by using an EXIF (Exchange Image File Format) viewer. URL: phishing detection engines will be used to check for its legitimacy Social networks analysis techniques could be used to determine relationships between social entities.
				To individual	Contact	Message content is safe
						Message has offensive/disruptive content
						Message has privacy related issues such as bank account number or photo of user's child
					Non-contact	Message content is safe
						Message has offensive/disruptive content
						Message has privacy related issues such as bank account number or photo of user's child
				To a group -- the user is alerted that group may contain non contacts as members		Message content is safe
						Message has offensive/disruptive content
						Message has privacy related issues such as bank account number or photo of user's child
		2	Share a document or location or contact or photo with	An individual	Contact	Whatapp does not have an API for developers. But one can query for `ContactsContract.RawContacts.ACCOUNT_TYPE` with value **`com.whatsapp.`** The recipient of this sharing is checked to see if contact or not and the user alerted. Another way for programmatically determining contacts in whatapp is as in http://stackoverflow.com/questions/35448250/how-
					Non-contact	
				A group -- the user is alerted that group may contain non contacts as members		

II. Application-related behaviors						
Category	**App**	**No.**	**Process**	**User behavior**	**How to monitor**	
					to-get-whatsapp-contact-from-android	
		3	Copy	Copying a message. No risk	TBC	
		4	Create group	Create a group of contacts and naming this group	TBC	
		5	Accept a group invitation (to become a group member)	From a contact	The contact number sending the invitation is checked against the contact list to determine if contact or not.	
				From a non-contact		
		6	Read messages	From a contact	TBC	
				From a non-contact		
		7	Delete	Delete a message.	TBC	
		8	Block contact	No risk	TBC	
		9	Star a message	Star a message to be stored as a favorite	TBC	
		10	Backup chats	Last backup	Local backups will run automatically every day at 2am and save your database in a file on the phone itself.	
				Google drive settings		
Email	**Gmail**	1	Sign in	Enter email address and password. Password could be weak, old or reused	A separate password table could be created for all app accounts. These passwords will be hashed and salted. Upon entry of password, various password defined- rules set could be checked using vt-password (passay) library which is	One or more password rule is violated

II. Application-related behaviors								
Category	**App**	**No.**	**Process**	**User behavior**			**How to monitor**	
							a password policy enforcement for JAVA. For example, HistoryRule is a rule for determining if a password matches one of any previous password a user has chosen. If no historical password reference has been set, then passwords will meet this rule.	All password rules are met
		2	Send email	To individual	Contact	With attachment	To programmatically determine user's Gmail contacts , the GData java client library for Google Contacts API could be used as in http://stackoverflow.com/questions/5125500/how-to-get-gmail-users-contacts Message/attachment content could contain anything from text, photos/videos, to URLs. For example, text message: depending on content of message. It could be offensive comments about disabilities, age, religious beliefs and sexual orientation. URL: could be of a phishing website Photos/videos: personal photo or video of children, credit card, military base …etc from camera or photo album that may include additional hidden info such as location. By the use of content filtering techniques, message content will be monitored to identify any disruptive, offensive message or personal information such as passwords or credit card numbers or if asking for personal information. A list of predefined black words or phrases could be	

II. Application-related behaviors							
Category	**App**	**No.**	**Process**	**User behavior**			**How to monitor**
							created, then by the implementation of a keystroke logger and text analysis the message content will be scanned against that list such that if any undesirable/risky content is detected it is picked up and flagged. For multimedia content: facial recognition techniques could be applied to determine persons in the file that might give rise to privacy related issues and user notified. Social networks analysis techniques could be used to determine relationships between social entities. Further to that, if a URL is included then it is checked for URL blacklists of malicious websites to check if it is a phishing URL (use a phishing detection engine).
						No attachment	To a contact (whether with or without attachment): Message content is safe
							Message has disruptive/offensive content
							Message has privacy related issues such as password, bank account number or user's child photo
					Non-contact	With attachment	whether with or without attachment: Message content is safe
							Message has disruptive/offensive content
							Message has privacy related issues such as password, bank account number or user's child photo
						No attachment	
				To group	With attachment		Whether with or without attachment: Message content is safe

II. Application-related behaviors						
Category	**App**	**No.**	**Process**	**User behavior**		**How to monitor**
						Message has disruptive/offensive content
						Message has privacy related issues such as password, bank account number or user's child photo
					No attachment	
				Sending a chain email.		Monitor content using a content filter that works against a list of words or phrases to identify such type of emails
		3	Read an email (text only) no attachments	From contact.		Whether from a contact or non-contact, The above mentioned techniques (as in send email) are used. The sender's email is checked for phishing and spoofing Message is safe
				From non-contact		Message has some safety issues
		4	Read an email with link/attachments	From contact.	Open/download with checking	The above mentioned techniques (as in send email) are used. The user is notified that the email has an attachment that has to be checked before opening it.
				From contact.	Open/download without checking	
				From a non-contact.	Open/download with checking	
				From a non-contact.	Open/download without checking	
		5	Reply	To Contact. Message content could contain anything from text, photos/videos, to URLs.	With attachment	As a precaution that the user may spread malicious emails whether intentionally or unintentionally or reply to a phishing email, the message content is checked such that there is no exposure of private information especially if the receiver is a non-contact. The above mentioned techniques (as in send email)
					Without attachment	

II. Application-related behaviors								
Category	**App**	**No.**	**Process**		**User behavior**			**How to monitor**
					Non-contact	With attachment		are used. If there is an attachment, then it is scanned for privacy related issues / malicious content
						Without attachment		
		6	Forward.		Contact.			Make sure the forwarded email is not an offensive or disruptive message such as a chain/phishing email using the techniques mentioned above
					Not a contact.			
		7	Delete		Delete an email			The Gmail API exposes the common Gmail labels on a message (like Starred and Unread), IMAP \Flagged maps to the Star in the web interface and "STARRED" in the API. The Important label (corresponding to the \Important mailbox in IMAP) should be visible in the in the API as well (system label called "IMPORTANT").If this is detected, then user is alerted
					Delete an email that was categorized as important.			
		8	Read sent items		No risk			TBC
		9	Settings	Download attachments	On. When On, it allows auto download of attachments (high risk)			The Gmail API could be used to determine settings in a GET request.
					Off			
Photos	**Google photos**	1	Remove location		On. A location is added to taken photos.	The system notifies the user of the consequences	OK	The method `IsProviderEnabled` of the class `LocationManager` provides access to the system location services. If the user has enabled this provider (`GPS_PROVIDER`, `NETWORK_PROVIDER`) in the Settings menu, true is returned otherwise false is returned. Moreover, geotagging info of a photo can be read from the EXIF header of the image file itself
					Off			

II. Application-related behaviors						
Category	**App**	**No.**	**Process**	**User behavior**	**How to monitor**	
		2	Back up	Create a backup of photos/videos album	Checking where they are stored in Google photos library i.e. Folder DCIM\camera (default storage) and check for `lastModified` date then compare it with today's date using the class `simpleDateFormat`	A recent backup is found
						An outdated back up is found
		3	Share	Sharing of photos with a contact/app.	Monitor for personal photo or video of children, credit card, military base …etc from camera or photo album that may include additional hidden info such as location. Facial detection and recognition techniques could be applied to determine persons in the file that might give rise to privacy related issues and user notified. Social networks analysis techniques could be used to determine relationships between social entities. Photo is safe	
					Photo has privacy related issues	
		4	Delete	Delete a copy	Traffic analysis	
		5	Add photo	Adding a photo to the photo album. The risk level depends on content of photo	Permissions and API calls tracing	
		6	Create album	Create an album of photos and naming it	Traffic analysis	

II. Application-related behaviors					
Category	**App**	**No.**	**Process**	**User behavior**	**How to monitor**
		7	Search/ Browse	Searching/ Browsing stored photos	Traffic analysis
Navigation	**Google maps**	1	Your places	Setting home address	If device is stolen, this info could be used to determine user's home and work address. User is notified of the consequences
				Setting work address	
		2	Your timeline	Add a photo to timeline	Permissions and API calls tracing. Facial detection and recognition techniques are used to scan the photo and alert the user if privacy related issues are detected. Photo is safe
					Photo has privacy related issues
		3	Write a review	Writing a review about a visited place	Traffic analysis
		4	Delete	Deleting a photo to a point of interest but not addresses or coordinates	Traffic analysis
		5	Add a photo	Adding a photo to a point of interest but not addresses or coordinates. Risk depends on photo content.	Permissions and API calls tracing. Facial detection and recognition techniques are used to scan the photo and alert the user if privacy related issues are detected. Photo is safe
					Photo has privacy related issues
		6	Share link	Share a location with contact/app	Social network analysis is used to determine relationships degrees.
		7	Get directions	Asking for directions to a certain destination	Traffic analysis
		8	Search	Search nearby places	Traffic analysis
		9	Read user's history	Reading places user been to	Traffic analysis
		10	Delete location history	Deleting of location history	Traffic analysis

II. Application-related behaviors						
Category	**App**	**No.**	**Process**	**User behavior**	**How to monitor**	
		11	Show traffic	Showing traffic on map	Traffic analysis	
News	**BBC News**	1	Read/watch/listen	Reading, watching or listening to BBC	Traffic analysis	
		2	Weather	Forecasting the weather	Traffic analysis	
		3	Search	Searching for specific news	Traffic analysis	
		4	Share	Share a link on BBC news with others	Content of what is being shared is monitored.	
Shopping	**Amazon**	1	Search	Search for certain products by typing its name	TBC	
				Search for certain products either by camera or scan	TBC	
		2	Create an account	Create an account on Amazon	Traffic analysis	
		3	Sign in	Enter email, name and password. Password could be weak/old/reused	A separate password table could be created for all app accounts. These passwords will be hashed and salted. Upon entry of password, various password defined-rules set could be checked using vt-password (passay) library which is a password policy enforcement for JAVA. For example, `HistoryRule` is a rule for determining if a password matches one of any previous password a user has chosen. If no historical password reference has been set, then passwords will meet this rule.	One or more password rule is violated
						All password rules are met

II. Application-related behaviors					
Category	**App**	**No.**	**Process**	**User behavior**	**How to monitor**
		4	Search orders	Searching of past orders by time/type	Traffic analysis
		5	View shopping list	Privacy settings: public, shared or private	Traffic analysis
		6	Delete list/ items from list	Deleting items from shopping list or the entire list	Traffic analysis
		7	Create shopping list (add items to shopping list)	Drag and drop items to shopping list	Traffic analysis
		8	Add/delete from cart	Adding/removing items from cart	Traffic analysis
		9	Create/add/ delete wish list	Creating a wish list of items, adding or deleting from it	Traffic analysis
		10	Proceed to check out	Enter shipping address	TBC
				Add a security access code	TBC
				Selecting shipping/ delivery options	TBC
				Add a credit or debit card (scanning or entering details)	Traffic analysis. The app itself is checked to see if it is updated or not. This could be done programmatically. Further to that if it is installed from official market app or not The `PackageManager` class supplies the `getInstallerPackageName` method that will return the package name of whatever installed the specified package. User will be notified of such information and alerted for consequences of entering such sensitive information. App is up to date and installed from official market
				Add a bank account	Either app is out of date, not installed from official market or both
		11	Share	Share a link with other contact/app	Traffic analysis
Music/video/audio	**YouTube**	1	Search	Searching for certain media	Traffic analysis
		2	Search history	Search previously watched videos	Traffic analysis
		3	Watch	Watching a video. Risk level depending on content of what is being watched	Content of video is monitored.
		4	add to watch later	Selecting a video for later viewing	
		5	Like/dislike	Selecting like or dislike for a certain file	
		6	Add a comment	Adding a comment to a certain video. Risk level depending on content of comment	Content of comment is scanned using previously mentioned techniques

II. Application-related behaviors					
Category	**App**	**No.**	**Process**	**User behavior**	**How to monitor**
					No issues found
					Disruptive/offensive content
					Privacy related issues
		7	Upload	Uploading a multimedia file.	Permissions and API call tracing
		8	Browse channels	Browsing channels on YouTube	Traffic analysis
		9	Subscribe	Subscribing to a certain channel. Risk level depends on type of channel	Suitability of channel could be determined by checking the About description of the channel. Or by using youtube analytics
		10	Unsubscribe	Unsubscribing from a certain channel.	Traffic analysis
		11	Trending	Browse what is trending	Traffic analysis
		12	Create a playlist	Create a play list of favorite videos	
		13	share	Share with a contact/app	Traffic analysis
Banking	**HSBC**	1	Read offers and rewards/read products and services	Browsing offers, products and services offered by bank	Traffic analysis.
		2	Fast balance	Choose account, Read the current balance without logging	Traffic analysis. User could be alerted that nobody is shoulder surfing or public wifi is used
		3	Find HSBC branch/ATM	Locating the nearest branch/ATM using Google map after giving it permission.	Traffic analysis
		4	Pay bill	Follow the on screen instructions to move money from current bank account to another selected account (bill account).	Traffic analysis. Checking if app is updated or not is done by the bank app itself. Type of internet connection (wifi or not) could be determined thru connectivityManager..if wifi is detected, security of such wifi could be determined programmatically using android.net.wifi package. In particular, the ScanResult.capabilities string will contain either 'WPA2', 'WPA' or 'WEP' if the hotspot is secured. User is alerted that he is attempting to perform a financial transaction. When selecting “confirm ” user should be notified as “are you sure??” No security issues found

II. Application-related behaviors						
Category	**App**	**No.**	**Process**	**User behavior**	**How to monitor**	
					Security issues found	
		5	Make Transfer	Follow the on screen instructions to move money from current bank account to another selected account.		
		6	Paym	Follow the on screen instructions to pay/transfer money from your account to the recipient's account using his mobile phone number only.		
		7	Secure message	Browse messages sent from bank	Traffic analysis	
		8	Logout	If not logout, it will automatically logout after 10 minutes of the app being idle, i.e. not used. Medium risk	TBC	
		9	Logon	Using two factor authentication. Either two passwords or a password and a secure key code. Password could be old/weak/reused	A separate password table could be created for all app accounts. These passwords will be hashed and salted. Upon entry of password, various password defined-rules set could be checked using vt-password (passay) library which is a password policy enforcement for JAVA. For example, HistoryRule is a rule for determining if a password matches one of any previous password a user has chosen. If no historical password reference has been set, then passwords will meet this rule.	One or more password rule is violated All password rules are met

Appendix D: Detailed Calculations of Software's Sum of CVSS scores According to Methodology Proposed by (Wu and Wang 2011)

- **For Operating system: Android V. 4.4.4:**
  Total number of vulnerabilities = 122.

Name of weakness	Number of vulnerabilities caused by this weakness
CWE 191	1
CWE 200	23**
CWE 399	4
CWE 284	19**
CWE 264	50**
CWE 119	4
CWE 20	3
CWE 388	1
CWE 190	3
CWE 254	1
CWE 275	1
CWE 19	4
CWE 74	1
CWE 89	1
CWE 22	1
CWE 362	1
CWE 189	3
CWE 476	1

** The top three weaknesses leading to most vulnerabilities, i.e representative weaknesses

CWE 264 = 50		CWE 200 = 23	
CVE ID	**CVSS BASE SCORE V2**	**CVE ID**	**CVSS BASE SCORE V2**
CVE-2017-0807	10.0	CVE-2017-0823	5.0
CVE-2017-0805	9.3	CVE-2017-0817	5.0
CVE-2017-0770	9.3	CVE-2017-0816	4.3
CVE-2017-0768	9.3	CVE-2017-0815	4.3
CVE-2017-0767	9.3	CVE-2017-0785	3.3
CVE-2017-0752	9.3	CVE-2017-0783	6.1
CVE-2017-0745	9.3	CVE-2017-0779	4.3
CVE-2017-0738	4.3	CVE-2017-0777	4.3
CVE-2017-0737	6.8	CVE-2017-0668	4.3
CVE-2017-0731	6.8	CVE-2017-0646	4.3
CVE-2017-0726	4.3	CVE-2017-0602	4.3
CVE-2017-0722	9.3	CVE-2017-0560	4.3

CVE-2017-0703	9.3	CVE-2017-0559	4.3
CVE-2017-0697	4.3	CVE-2017-0558	4.3
CVE-2017-0694	4.3	CVE-2017-0547	4.3
CVE-2017-0692	4.3	CVE-2017-0425	4.3
CVE-2017-0690	4.3	CVE-2017-0420	4.3
CVE-2017-0681	9.3	CVE-2017-0398	4.3
CVE-2017-0671	9.3	CVE-2017-0397	4.3
CVE-2017-0666	9.3	CVE-2017-0396	4.3
CVE-2017-0665	9.3	CVE-2015-6644	4.3
CVE-2017-0644	7.1	CVE-2015-5310	3.3
CVE-2017-0641	7.1	**CVSS SUM =**	**100.1**
CVE-2017-0600	7.1	**CWE 284 = 19**	
CVE-2017-0597	9.3	**CVE ID**	**CVSS BASE SCORE V2**
CVE-2017-0596	9.3	CVE-2017-0814	7.8
CVE-2017-0595	9.3	CVE-2017-0809	9.3
CVE-2017-0594	9.3	CVE-2017-0782	8.3
CVE-2017-0554	6.8	CVE-2017-0781	8.3
CVE-2017-0546	9.3	CVE-2017-0775	7.1
CVE-2017-0544	9.3	CVE-2017-0774	7.1
CVE-2017-0481	9.3	CVE-2017-0766	9.3
CVE-2017-0480	9.3	CVE-2017-0764	9.3
CVE-2017-0479	9.3	CVE-2017-0756	9.3
CVE-2017-0475	9.3	CVE-2017-0714	9.3
CVE-2017-0419	9.3	CVE-2017-0713	6.8
CVE-2017-0418	9.3	CVE-2017-0663	6.8
CVE-2017-0417	9.3	CVE-2017-0491	4.3
CVE-2017-0416	9.3	CVE-2017-0489	4.3
CVE-2017-0395	4.3	CVE-2017-0393	7.1
CVE-2017-0385	9.3	CVE-2017-0392	7.1
CVE-2017-0384	9.3	CVE-2017-0390	7.1
CVE-2015-6645	7.1	CVE-2016-6770	4.3
CVE-2015-6640	9.3	CVE-2016-6763	7.1
CVE-2015-6637	9.3	**CVSS SUM =**	**140.0**
CVE-2014-8610	3.3		
CVE-2014-8609	7.2		
CVE-2014-7921	10		
CVE-2014-7920	10		
CVE-2014-7911	7.2		
CVSS SUM =	**398.4**		

CWE ID	# Vul. (K)	Time span in months (M)	Prob. Of vul. Occurrence (Rn) = K/M	Severity of weakness (Wn) = sum of vul/#vul	Percentage of each weakness in sw (Pn)=Rn/sum of R
CWE 264	50	12/2014-10/2017, M=34	50/34=1.47	398.4/50 = 7.97	1.47/4.67 = 0.315
CWE 200	23	1/2016-10/2017, M=21	23/21= 1.09	100.1/23 = 4.35	1.09/4.67 = 0.233
CWE 284	19	1/2017-10/2017, M=9	19/9=2.11	140/19 = 7.37	2.11/4.67 = 0.452

- **For applications:**

a) **Google Chrome for Android v. 39.0.2171.45 :**
Total number of vulnerabilities = 1

CWE 284 = 1	
CVE ID	**CVSS BASE SCORE V2**
CVE-2014-7905	5.0
CVSS SUM =	**5.0**

** Only one weakness found, thus considered as the representative weakness

b) **Google Email Application v. 4.2.2.0200 :**
Total number of vulnerabilities = 1

CWE 19 = 1	
CVE ID	**CVSS BASE SCORE V2**
CVE-2015-1574	5.0
CVSS SUM =	**5.0**

** Only one weakness found, thus considered as the representative weakness

c) **Symantec Mobile Security v. 1.0 :**
Total number of vulnerabilities = 1

CWE 255 = 1	
CVE ID	**CVSS BASE SCORE V2**
CVE-2010-0113	4.3
CVSS SUM =	**4.3**

** Only one weakness found, thus considered as the representative weakness

CWE ID	# Vul. (K)	Time span in months (M)	Prob. Of vul. Occurrence (Rn) = K/M	Severity of weakness (Wn)= sum of vul/#vul	Percentage of each weakness in sw (Pn)=Rn/sum of R
a) Google Chrome for Android v. 39.0.2171.45:					
CWE 284	1	11/2014-9/2017, M=34	1/34=0.029	5.0/1=5.0	0.029/0.029=1
b) Google Email Application v. 4.2.2.0200:					
CWE 19	1	2/2015-2/2015, M=1	1/1=1	5.0/1=5.0	1/1=1
c) Symantec Mobile Security v. 1.0					
CWE 255	1	11/2010-8/2017, M=81	1/81=0.01	4.3/1=4.3	0.01/0.01=1

- **For Network Router CISCO AIRONET access point software ver. 8.1 (112.3):**
  Total number of vulnerabilities = 3

Name of weakness	Number of vulnerabilities caused by this weakness
CWE 119	1
CWE 264	1
CWE 20	1

** Only three weaknesses found, thus considered as the representative weaknesses

CWE 119 = 1		CWE 264 = 1		CWE 20 = 1	
CVE ID	**CVSS BASE SCORE V2**	**CVE ID**	**CVSS BASE SCORE V2**	**CVE ID**	**CVSS BASE SCORE V2**
CVE-2016-6363	6.1	CVE-2016-6362	7.2	CVE-2016-6361	6.1
CVSS SUM =	**6.1**	**CVSS SUM =**	**7.2**	**CVSS SUM =**	**6.1**

CWE ID	# Vul. (K)	Time span in months (M)	Prob. Of vul. Occurrence (Rn) = K/M	Severity of weakness (Wn)= sum of vul/#vul	Percentage of each weakness in sw (Pn)=Rn/sum of R
CWE 119	1	8/2016-12/2016, M=4	1/4=0.25	6.1/1=6.1	0.25/0.75 = 0.33
CWE 264	1	8/2016-12/2016, M=4	1/4=0.25	7.2/1=7.2	0.25/0.75 = 0.33
CWE 20	1	8/2016-12/2016, M=4	1/4=0.25	6.1/1=6.1	0.25/0.75 = 0.33

References

Abawajy, J. (2012) User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3), pp. 237-248.

Al Sabbagh, B., Ameen, M., Watterstam, T., and Kowalski, S. (2012) A Prototype for HI2 Ping information security culture and awareness training. In: *(ICEEE) International Conference on e-learning and e-Technologies in Education*. 2012, IEEE, pp. 32 - 36.

Alarifi, A., Tootell, H., and Hyland, P. (2012) A Study of information security awareness and practices in Saudi Arabia. In: *(ICCIT 2012) The 2nd International Conference on Communication and Information Technology*. 2012, IEEE, pp. 6 - 12.

AlAwawdeh, S. and Tubaishat, A. (2014) An Information Security Awareness Program to Address Common Security Concerns in IT Unit. In: *11th International Conference on Information Technology: New Generations (ITNG)*. 2014, pp. 273-278.

Albrechtsen, E. (2007) A qualitative study of users' view on information security. *Computers & Security*, 26(4), pp. 276-289.

Albrechtsen, E. and Hovden, J. (2010) Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, 29(4), pp. 432-445.

Alguliev, R., Derakhshandeh, S., and Imamverdiyev, Y. (2009) Information Security Risk Assessment Using Baysian Networks. In: *International Conference on Application of Information and Communications Technologies (AICT)*. 2009, pp. 1-4.

Al-Hadadi, M. and Al Shihani, A. (2013) Smartphone security awareness: Time to act. In: *(CTIT) International Conference for Current Trends in Information Technology*. 2013, IEEE, pp. 166 - 171.

Allam,S., Flowerday, S. and Flowerday, E. (2014) Smartphone information security awareness: A victim of operational pressures. *Computers and Security*, 42, pp. 56-65.

Allodi, L. and Massacci, F. (2012) A preliminary analysis of vulnerability scores for attacks in wild: the Ekits and sym datasets. In: *Proceedings of the 2012 ACM Workshop on Building Analysis Datasets and Gathering Experience Returns for Security,*. 2012, ACM, pp. 17-24.

Allodi, L. and Massacci, F. (2014) Comparing Vulnerability Severity and Exploits Using Case-Control Studies. *ACM Transactions on Information and System Security*, 17(1), pp. 1-20.

Allodi, L., Shim, w., and Massacci, F. (2013) Quantitative assessment of risk reduction with cybercrime black market monitoring. In: *IEEE Security and Privacy Workshops*. 2013, IEEE, pp. 165-172.

Alotaibi, F., Clarke, N. and Furnell, S. (2017) An analysis of home user security awareness & education. In:*12th International Conference for Internet Technology and Secured Transactions (ICITST)*, Cambridge, 2017, pp. 116-122.

Aloul, F. (2010) Information Security Awareness in UAE: A survey paper. In: *(ICITST) International Conference for Internet Technology and Secured Transactions*. 2010, IEEE, pp. 1 - 6.

Alsaleh, M. and Alshaer, E. (2014) Enterprise Risk Assessment Based on Compliance Reports and Vulnerability Scoring Systems. In: *Proceedings of the 2014 Workshop on Cyber Security Analytics, Intelligence and Automation (SafeConfig)*. 2014, pp. 25-28.

Amankwa, E., Loock, M., and Kritzinger, E. (2014) A conceptual analysis of information security education, information security training and information security awareness definitions. In: *(ICITST 2014) The 9th International Conference for Internet Technology and Secured Transactions*. 2014, IEEE, pp. 248 - 252.

Asgharpor, F., Liu, D., and Camp, L. (2007) Mental models of computer security risks. In: *Sixth Workshop on Economics of Information Security.*. 2007, pp. 1 - 9.

Adelola, T., Dawson, R. and Batmaz, F (2015) The urgent need for an enforced awareness programme to create internet security awareness in Nigeria. In: *Proceedings of the 17th International Conference on Information Integration and Web-based Applications & Services* (iiWAS'15), 2015, ACM, Article No.82.

Ahmed, Y., Ahmad, M., Ahmad, N. and Zakaria, N. (2018) Social media for knowledge-sharing: A systematic literature review. *Telematics and Informatics*, ELSEVIER.

Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S. and Reich, C. (2015) Security, privacy and usability–a survey of users' perceptions and attitudes. In: *12th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2015).* 2015, Springer International Publishing, Vol.9264 of the series Lecture Notes in Computer Science, pp. 153-168

Bachrach, Y., Kosinski, M., and Graepel, T. (2012) Personality and Patterns of Facebook Usage. In: *WebSci 2012*. 2012, Evanston, Illinois, USA: ACM.

Badie, N. and Lashkari, H. (2012) A New evaluation criteria for effective security awareness in computer risk management based on AHP. *Journal of Basic and Applied Scientific Research*, 2(9), pp. 9331 - 9347.

Bergomi, F., Paul, S., Solhaug, B., and Vignon-Davillier, R. (2013) Beyond Traceability: Compared Approaches to Consistent Security Risk Assessments. In: *2013*, *International Conference on Availability, Reliability and Security*, pp. 814-820.

Bhattacharjee, J., Sengputa, A., and Mazumdar, C. (2013) A Formal Methodology for Enterprise Information Security Risk Assessment. In: *International Conference on Risks and Security of Internet and Systems (CRISIS)*. 2013, pp. 1-9.

Bhattacharjee, J., Sengputa, A., Mazumdar, C., and Barik, M. (2012) A two-phase Quantitative Methodology for Enterprise Information Security Risk Analysis. In: *CUBE*. 2012, ACM, pp. 809-

815.

Blythe, J. and Camp, L. (2012) Implementing mental models. In: *Security and Privacy Workshops*. 2012, IEEE, pp. 86 - 90.

Blythe, J., Camp, J., and Garg, (2011) Targeted risk communication for computer security. In: *IUI' 11*. 2011, ACM, pp. 295 - 298.

Bojanc, R. and Jerman-Bla¦¾iچؤ, B. (2013) A Quantitative Model for Information-Security Risk Management. *Engineering Management Journal*, 25(2), pp. 25-37.

Bostan, A. and Akman, I. (2013) ICT User and usage characteristics and e-mail security awareness. In: *(ICECCO) International Conference on Electronics, Computer and Computation*. 2013, IEEE, pp. 277 - 280.

Bonneau, J. (2012) The Science of Guessing Analyzing an Anonymized Corpus of 70 Million Passwords. *IEEE Symposium on Security and Privacy*, San Francisco, California.

Butler, R. and Butler, MJ (2014) An Assessment of the Human Factors Affecting the Password Performance of South African Online Consumers. In: *Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA, 2014)*, 8-10 July, Plymouth UK, pp150-161

Camp, L. (2006) Mental models of privacy and security. *IEEE Technology and Society Magazine*, 28(3), pp. 37-46.

Clarke, N., Li, F., Furnell, S., Stengel, I., Ganis, G. (2016) Information Security and Practice: The User's Perspective. In: *Proceedings of the 11th International Conference On Cyber Warfare and Security (ICCWS-2016)*. 2016, Boston, USA, pp.81-89.

Coeffield, F., Moseley, D., Hall, E., and Ecclestone, K. (2004) *Learning styles and pedagogy in post-16 learning: A Systematic and critical review*. Learning and Skills Research Centre.

Community Norton Protection . Available at https://community.norton.com/en/blogs/norton-protection-blog/how-safe-surfing-4g-vs-wi-fi. Accessed 26 December 2016.

Cone, B., Irvine, C., Thompson, M., and Nguyen, T. (2007) A video game for cyber security training and awareness. *Computers & Security*, 26(1), pp. 63-72.

CORAS*, The CORAS Method* (n.d.) [Online]. Available at: http://coras.sourceforge.net. (Accessed: 15 December 2014).

CPE [Online]. Available at: http://nvd.nist.gov/cpe.cfm. (Accessed: 4 February 2016)

CVE [Online]. Available at: http://cve.mitre.org. (Accessed: 30 March 2016).

Cyber Street | Protect your home or business from cybercrime (2015) [Online]. 2015. Available at: http://cyberstreetwise.com. (Accessed: 6 May 2015).

Cetto, A., Netter, M., Pernul, G., Richthammer, C., Riesner, M., Roth, C., and Sänger, J. (2014). Friend Inspector: A Serious Game to Enhance Privacy Awareness in Social Networks. In: *2nd International Workshop on Intelligent Digital Games for Empowerment and Inclusion (IDGEI)*, 2014.

Chaisiri, S., Ko, R. and Niyato, D. (2015) A Joint Optimization Approach to Security-as-a-Service Allocation and Cyber Insurance Management. In: *IEEE Trustcom/BigDataSE/ISPA*. 2015, IEEE, pp. 426-433.

Chan, R., Ho, K., Jia, S., Wang, Y., Yan, X. and X. Yu (2016) Facebook and information security education: What can we know from social network analyses on Hong Kong engineering students?. In:*IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 2016, IEEE, pp. 303-307.

Chawla, S. and Thamilarasu, G. (2018) Security as a service: real-time intrusion detection in internet of things. In: *Proceedings of the Fifth Cybersecurity Symposium (CyberSec '18)*. 2018, ACM, Article No.12

Chen, w., Shariah, S. and Blainey, B. (2018) A security-as-a-service solution for applications in cloud computing environment. In: *Proceedings of the Communications and Networking Symposium (CNS '18)*. 2018, Society for Computer Simulation International, Article No.4.

Cloud Security Alliance Security as a Service Work Group. Available in <https://cloudsecurityalliance.org/working-groups/security-as-a-service/#_overview>. [24 December 2018]

Egelman, S. and Peer, E. (2015) (a) Predicting privacy and security attitudes. *SIGCAS Comput. Soc.*, 45(1), pp. 22-28.

Egelman, S. and Peer, E. (2015) (b) The Myth of The Average User. In: *NSPW'15*. 2015, Twente, Netherlands: ACM.

ENISA, (2010) *The new users' guide: How to raise information security awareness*. European Network and Information Security Agency.

European Agency For Network and Information Security (ENISA), (n.d.) *Inventory of Risk Management- Risk Assessment Methods and Tools*. [Online]. Available at: http://rm-inv.enisa.europa.eu/methods. (Accessed: 24 December 2014).

Erdem, E. and Sandıkkaya, M. (2019) OTPaaS—One Time Password as a Service. *IEEE Transactions on Information Forensics and Security*, Vol. 14, No. 3, pp. 743-756.

Fard, M. and Wang, K. (2015) Neighborhood randomization for link privacy in social network analysis. *World Wide Web*, Vol.8, No.1, pp.9-32.

Feng, N., Wang, H., and Li, M. (2014) A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Information Sciences*, 256, pp. 57-73.

Fillipidis, A., Hilas, C., Fillipidis, G.and Politis, A. (2018) Information security awareness of Greek higher education students- preliminary findings. In: (MOCSAT) 7th International conference on modern circuits and systems technologies, IEEE, 7-9 May, Greece, pp. 1-4.

Fleming, N. (2001) *Teaching and learning styles*. Christchurch, N.Z.: Neil Fleming.

Furnell, S. and Clarke, N. (2012) Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, 31(8), pp. 983-988.

Furnell, S. and Moore, L. (2014) Security literacy: the missing link in today's online society?. *Computer Fraud & Security*, 2014(5), pp. 12-18.

Furnell, S. and Rajendran, A. (2012) Understanding the influences on information security behavior. *Computer Fraud and Security*, (March 2012), pp. 12-15.

Furnell, S. and Thomson, K. (2009) From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security*, 2009(2), pp. 5-10.

Furnell, S., Bryant, P., and Phippen, A. (2007) Assessing the security perceptions of personal Internet users. *Computers & Security*, 26(5), pp. 410-417.

Furnell, S., Tsaganidi, V., and Phippen, A. (2008) Security beliefs and barriers for novice Internet users. *Computers & Security*, 27(7-8), pp. 235-240.

Gabriel, T. and Furnell, S. (2011),"Selecting security champions", *Computer Fraud & Security*, Vol.8, pp.8-12

Gartner.com *Gartner Says Emerging Markets Drove Worldwide Smartphone Sales to 19 Percent Growth in First Quarter of 2015* (2016) [Online]. 2016. Available at: http://www.gartner.com/newsroom/id/3061917. (Accessed: 10 December 2015).

Get Safe Online | *Free online security advice* (2015) [Online]. 2015. Available at: http://getsafeonline.org. (Accessed: 15 May 2015).

Gros, S. (2011) Complex Systems and Risk Management. In: *MIPRO*. 2011, pp. 1522-1527.

Gosling, S.D, Rentfrow, P.J and Swann, W.B. (2003), "A very brief measure of the Big-Five personality domains", *Journal of Research in Personality*, Vol.37 No.6, pp. 504–528.

General Data Protection Regulation (GDPR). Available from: https://gdpr-info.eu/. [2 January 2019]

Goode, S., Lin, C., Tsai, J. and Jiang, J. (2015) Rethinking the role of security in client satisfaction with Software-as-a-Service (SaaS) providers. *Decision Support Systems*, Vol.70, pp.73-85.

Gritzalis, D., Iseppi, G, Mylonas, A. and Stavrou, V. (2018) Exiting the Risk Assessment Maze: A Meta-Survey, *ACM Computing Surveys,* Vol.51, No.1, pp.1-30

Halevi, T., Lewis, J., and Memon, N. (2013) A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits. In: *International World Wide Web Conference (IW3C2)*. 2013, Rio de Janero, Brazil: ACM, pp. 737-744.

Hansch, N. and Benenson, Z. (2014) Specifying IT security awareness. In: *25th International Workshop on Database and Expert Systems Applications*. 2014, IEEE, pp. 326 - 330.

Harbach, M., Fahl, S., and Smith, M. (2014) Who's afraid of which bad wolf? A survey of IT security risk awareness. In: *27th Computer Security Foundations Symposium*. 2014, IEEE, pp. 97 - 110.

Hargreaves, D. (2005) *About learning: report of the Learning Working Group*. Demos.

Hasan, M. and Moftah, H. (2013) Cloud-based security services for the smart grid. In: *Proceedings of the 2013 Conference of the Center for Advanced Studies on Collaborative Research (CASCON '13)*. 2013, IBM Corp, pp. 388-391.

Hussain, M. and Abdulsalam, H. (2011) SECaaS: security as a service for cloud-based applications. In: *Proceedings of the Second Kuwait Conference on e-Services and e-Systems (KECESS '11)*, 2011, ACM, Article No.8.

Hasan, M. and Hussin, H. (2010) Self-awareness before social networking: Exploring the user behavior and information security vulnerability in Malaysia. In: *3rd International Conference on ICT4M*. 2010, pp. 7 - 12.

Helkala, K. and Bakas, T.H. (2013), "National Password Security Survey: Results", in *Proceedings of the European Information Security Multi-Conference (EISMC 2013*) *in Lisbon, Portugal*, University of Plymouth Press, pp23-24

Herath, T. and Rao, H. (2009), "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18 No.2, pp. 106-125

Holm, H. and Afridi, K. (2015) An expert-based investigation of the Common Vulnerability Scoring System. *Computers & Security*, 53, pp. 18-30.

Holm, H., Ekstedt, M., and Andersson, D. (2012) Empirical Analysis of System-Level Vulnerability Metrics through Actual Attacks. *IEEE Transactions on Dependable and Secure Computing*, 9(6), pp. 825-837.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012), "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture", *Decision Sciences*, Vol.43 No.4, pp.615–660.

Ibrahim, T., Furnell, S., Papadaki, S., and Clarke, N. (2010) Assessing the Usability of End-user Security Software. In: *Proceedings of the 7th International Conference, TrusBus*. 2010.

Imamverdiyev, Y. (2013) An Application of Extreme Value Theory to e-Government Information Security Risk Assessment. In: *7th International Conference On Application of Information and*

Communication Technologies (AICT). 2013, pp. 1-4.

Internet Access - Households and Individuals, 2013 - *ONS* (2013) [Online]. 2013. Available at: http://www.ons.gov.uk/ons/rel/rdit2/internet-access---households-and-individuals/2013/index.html. (Accessed: 15 November 2015).

Imran-Daud, M., Snchez, D. and Viejo, A. (2016) Privacy-driven Access Control in Social Networks by Means of Automatic Semantic Annotation. *Computer Communications*, Vol. 76, pp. 12-25.

Jain, M. and Clarke, N. (2010) Web-Based Risk Analysis for Home Users. *Advances in Communications, Computing, Networks and Security*, 7, pp. 151-158.

Jeske, D., Coventry, L., Briggs, P., and Moorsel, A. (2014) Nudging whom how: IT proficiency, impulse control and secure behavior. *Networks*, 49(18).

Jing, Y., Ahn, G., Zhao, Z., and Hu, H. (2014) RiskMon: Continuous and Automated Risk Assessment of Mobile Applications. In: *Proceedings of The 4th Conference on Data and Application Security and Privacy*. 2014, ACM, pp. 99-110. Karabacak, B. and Sogukpinar, I. (2005) ISRAM: information security risk analysis method. *Computers & Security*, 24(2), pp. 147-159.

John, O. and Srivastava, S. (1999) *The Big-Five trait taxonomy: History, measurement, and theoretical perspectives*.

Johnston, A., Warkentin, M., McBride, M. and Carter, L. (2016), "Dispositional and situational factors: influences on information security policy violations", *European Journal of Information Systems,* Vol.25 No.3, pp.231–251

Kajzer, M., D'Arcy, J., Crowell, C., Striegel, A., and Van Bruggen, D. (2014) An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers & Security*, 43, pp. 64-76.

Karabacak, B. and Sogukpinar, I. (2005) ISRAM: Information Security Risk Analysis method. *Computers and Security*, 24(2), pp. 147-159

Kaspersky, (2016) *Kaspersky security bulletin 2013*. Kaspersky Labs.

Kaspersky, (2017) *Kaspersky security bulletin 2014*. Kaspersky Labs

Kaur, J. and Mustafa, N. (2013) Examining the effects of knowledge, attitude and behavior on information security awareness: A Case on SME. In: *(ICRIIS'13) 3rd International Conference on Research and Innovation in Information Systems*. 2013, pp. 286 - 290.

Khan, B., Alghathbar, K., Nabi, S., and Khan, M. (2011) Effectiveness of information security awareness methods based on psychological theories. *AFRICAN JOURNAL OF BUSINESS MANAGEMENT*, 5(26), pp. 10862- 10868.

Komatsu, A., Takagi, D., and Takemura, T. (2013) Human aspects of information security.

Information Management & Computer Security, 21(1), pp. 5-15.

Kritzinger, E. and von Solms, S. (2010) Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 29(8), pp. 840-847.

Kritzinger, E. and Von Solms, S. (2013) Home user security from thick security-oriented home users to thin security-oriented home users. In: *Science and Information Conference*. 2013, pp. 340 - 345.

Kruger, H., Flowerday, S., Drevin, L., and Steyn, T. (2011) An assessment of the role of cultural factors in information security awareness. In: *(ISSA) Information Security South Africa*. 2011, IEEE, pp. 1 - 7.

Karavaras, E., Magkos, E. and Tsohou, A. (2016) Low User Awareness Against Social Malware: An Empirical Study and Design of a Security Awareness Application. In: *13th European Mediterranean & Middle Eastern Conference on Information Systems (EMCIS 2016)*. 2016, pp. 1–10.

Kim, G., An, J. and Kim, K. (2017) A study on authentication mechanism in SEaaS for SDN. In: *Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication (IMCOM '17)*. 2017, ACM, Article No.51.

Kim, J., Hong, S., Min, J. and Lee, H. (2011) Antecedents of application service continuance: A synthesis of satisfaction and trust. *Expert Systems with Applications: An International Journal*, Vol. 38, No.8, pp.9530-9542.

Lebek, B., Uffen, J., Breitner, M., Neumann, M., and Hohler, B. (2013) Employees' information security awareness and behavior: A Literature Review. In: *46th Hawaii International Conference on System Sciences*. 2013, IEEE, pp. 2978 - 2987.

Ledermuller, T. and Clarke, N. (2011) Risk Assessment for Mobile Devices. *Lecture Notes in Computer Science*, 6863, pp. 210-221.

Liu, Q. and Zhang, Y. (2011) VRSS: A new system for rating and scoring vulnerabilities. *Computer Communications*, 34(3), pp. 264-273.

Lynam, D. R. and Widiger, T. A. (2001), "Using the five-factor model to represent the DSM-IV personality disorders: An expert consensus approach", *Journal of Abnormal Psychology*, Vol.110 No.3, pp.401–412.

Labuschagne, W., Burke, I, Veerasamy, N. and Eloff, M (2011) Design of cyber security awareness game utilizing a social media framework. *Information Security for South Africa*, Johannesburg, 2011, pp. 1-9.

Laleh, N., Carminati, B. and Ferrari, E. (2018) Risk Assessment in Social Networks Based on User Anomalous Behaviors. *IEEE Transactions on Dependable and Secure Computing*, Vol.15, No.2, pp.295-308.

Li, L. and Qian, K. (2016) Using Real-Time Fear Appeals to Improve Social Media Security. In: *40th Annual Computer Software and Applications Conference (COMPSAC)*, 2016, IEEE, pp.610-611.

Liu, F., Pan, L. and Yao, L. (2018) Evolutionary Game Based Analysis for User Privacy Protection Behaviors in Social Networks. In: (DSC) *Third International Conference on Data Science in Cyberspace*, 2018, IEEE, pp. 274-279.

Magerit, (2006) *Methodology for Information Systems Risk Analysis and Management: Book 1-The Method*. Madrid: Ministerio de Administracones Publicas.

Martin, N. and Rice, J. (2011) Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security*, 30(8), pp. 803-814.

Maurer, M., De Luca, A., and Kempe, S. (2011) Using data type based security alert dialogs to raise online security awareness. In: *SOUPS' 2011*. 2011, pp. 1 - 13.

McAfee Official US Store - Latest 2015 Edition (2015) [Online]. 2015. Available at: http://home.mcaffee.com/advicecenter. (Accessed: 30 April 2015).

McBride, M., Carter, L. and Warkentin, M. (2012) Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies, RTI International-Institute for Homeland Security Solutions

Mehari, (2007) Overview. *Club de la Securite de I'Information Francis (CLUSIF)*,

Mell, P., Scarfone, K., and Romanosky, S. (2007) *CVSS: a complete guide to the common vulnerability scoring system version 2.0*. [Online]. 2007. Available at: http://first.org/cvss/cvss-guide.html. (Accessed: 18 February 2016).

Mensch, S. and Wilkie, L. (2011) Information Security Activities of College Students: An Exploratory Study. *Academy of Information and Management Sciences*, 14(2), pp. 91-116.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., and Giannakopoulos, G. (2014) The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia - Social and Behavioral Sciences*, 147, pp. 424-428.

Microsoft Internet Safety and Security Center (2015) [Online]. 2015. Available at: http://microsoft.com/security/default.aspx. (Accessed: 5 May 2015).

MehariPedia. Available from: < http://meharipedia.x10host.com/wp/home/>. [5 January 2019].

Mendel, E. and Toch, E. (2017) Susceptibility to Social Influence of Privacy Behaviors: Peer versus Authoritative Sources. In: *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (CSCW'17), 2017, ACM, pp.581-593.

Moyo, M., Abdullah, H., and Nienaber, R. (2013) Information Security Risk Management in Small-scale Organizations: A Case Study of Secondary Schools Computerized Information Systems. In: *Conference of Information Security for South Africa*. 2013, pp. 1-6.
Mylonas, A., Kastania, A., and Gritzalis, D. (2013) Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, 34, pp. 47-66.

National Cyber Security Alliance | *StaySafeOnline.org* (2015) [Online]. 2015. Available at: http://staysafeonline.org. (Accessed: 19 May 2015).

National Institute of Standards and Technology NIST Special Publication 800-30, Revision 1, (2012) *Guide for Conducting Risk Assessment*.

NIST SP 800-16, (1998) *Information technology training requirements: A Role-and performance based model*. National Institute of Standards and Technology (NIST).

NIST, (2013) *US National vulnerability database*. [Online]. 2013. Available at: http://nvd.nist.gov. (Accessed: 18 February 2016).

Number of Internet Users (2017) - Internet Live Stats (2017) [Online]. 2017. Available at: http://internetlivestats.com/internet-users/. (Accessed: 1 August 2017).

Number of worldwide social network users 2010-2018 | Statistic (2016) [Online]. 2016. Available at: http://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/. (Accessed: 29 October 2015).

OCTAVE Available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html. Accessed: 21 December 2014.

Oliveira, R., Cherubini, M., and Oliver, N. (2013) Influence of personality on satisfaction with mobile phone services. *ACM Transactions on Computer-Human Interaction*, 20(2), pp. 1-23.

Olusegun, O. and Ithnin, N. (2013) People are the answer to security: Esatblishing a sustainable Information Security Awareness Training (ISAT). *International Journal of Computer Science and Information Security*, 11(8).

Ophoff, J. and Robinson, M. (2014) Exploring end-user smartphone security awareness within a South African context. In: *(ISSA) Information Security for South Africa*. 2014, IEEE, pp. 1 - 7.

OVAL [Online]. Available at: http://oval.mitre.org. (Accessed: 25 March 2016).

Paintsil, E. (2012) Taxonomy of Security Risk Assessment Approaches for Researchers. In: *4th International Conference on Computational Aspects of Social Networks (CASoN)*. 2012, pp. 257-262.

Panda, P. (2009) The OCTAVE Approach to Information Security Risk Assessment. *ISACA*, [Online]. 4. Available at: http://esl.dk/media/1094/jpdf094-the-octave.pdf. (Accessed: 8 January 2015).

Paul, S. and Vignon-Davillier, R. (2014) Unifying traditional risk assessment approaches with attack trees. *Journal of Information Security and Applications*, 19(3), pp. 165-181.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., and Butavicius, M. (2012) Why do some people manage phishing e-mails better than others?. *Information Management & Computer Security*, Vol. 20 No.1, pp. 18 – 28

Pirzadeh, L. and Jonsson, E. (2011) A Cause and Effect Approach Towards Risk Analysis. In: *Third International Workshop on Security Measurements and Metrics*. 2011, pp. 80-83.

Poolsappasit, N., Dewri, R., and Ray, I. (2012) Dynamic Security Risk Management Using Bayesian Attack Graphs. *IEEE Transactions on Dependable and Secure Computing*, 9(1), pp. 61-74.

Pang, J. and Zhang, Y. (2014) A New Access Control Scheme for Facebook-Style Social Networks. In: *Ninth International Conference on Availability Reliability and Security*, 2014, IEEE, pp. 44-59.

Rajabhandari, L. (2013) Consideration of Opportunity and Human Factor: Required Paradigm Shift for Information Security Risk Management. In: *European Intelligence and Security Informatics Conference*. 2013, pp. 147-150.

Rakic-Bajic, G. and Hedrih, V. (2012) Excessive use of the Internet, life satisfaction and personality factors. *Suvren Psihol*, 15(1), pp. 119 - 130.

Rao, U. and Pati, B. (2012) Study of Internet security threats among home users. In: *Fourth International Conference on Computational Aspects of Social Networks*. 2012, IEEE, pp. 217 - 221.

Rughinis, C. and Rughinis, R. (2014) Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union. *Computers & Security*, 43, pp. 111-125.

Sadiq, M., Ahmad, M., Rahmani, K., and Jung, S. (2010) Software Risk Assessment and Evaluation Process Using Model-Based approach. In: *International conference on Networking and Information Technology*. 2010, pp. 171-177.

Saleh, M. and Alfantookh, A. (2011) A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics*, 9(2), pp. 107-118.

Samy, G., Ahmad, R., and Ismail, Z. (2010) A Framework for Integrated Risk Management Process Using Survival Analysis Approach in Information security. In: *6th International Conference on Information assurance and Security*. 2010, pp. 185-190.

Sari, P. and Prasetio, A. (2017) Knowledge sharing and electronic word of mouth to promote information security awareness in social network sites. In: (IWBIS) International workshop on big data and information security, IEEE, pp. 113-117

Sedinic, I., Lovric, Z., and Perusic, T. (2014) Customer and user education as a tool to increase security level. In: *MIPRO 2014*. 2014, pp. 1441 - 1445.

Sharma, D., Dhote, C. and Potey, M. (2016) Identity and Access Management as Security-as-a-Service from Clouds. *Procedia Computer Science*, Volume 79, pp.170-174.

Shillair, R. (2016) Talking about Online Safety: A Qualitative Study Exploring the Cybersecurity Learning Process of Online Labor Market Workers. In: *Proceedings of the 34th ACM International Conference on the Design of Communication (SIGDOC '16)*. 2016, ACM, Article No.21.

Shamala, P., Ahmad, R., and Yusoff, M. (2013) A conceptual framework of info structure for information security risk assessment (ISRA). *Journal of Information Security and Applications*, 18(1), pp. 45-52.
Shaw, R., Chen, C., Harris, A., and Huang, H. (2009) The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52(1), pp. 92-100.

Shedden, P., Scheepers, R., Smith, W., and Ahmad, A. (2011) Incorporating a knowledge perspective into security risk assessments. *VINE*, 41(2), pp. 152-166.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., and Downs, J. (2010) Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of intervensions. In: *CHI 2010: Privacy Behaviors*. 2010, ACM, pp. 373 - 382.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J., and Nunge, E. (2007) AntiPhishing Phil: The design and evaluation of a game that teaches people not to fall for Phish. In: *(SOUPS) 3rd Symposium on Usable Privacy and Security*. 2007, ACM, pp. 88 - 99.

Shillair, R., Cotten, S., Tsai, H., Alhabash, S., LaRose, R., and Rifon, N. (2015) Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, 48, pp. 199-207.

Schuessler, J.H. and Hite, D.M. (2014) Pre-Employment Screening for Security Risk: An Exploratory Study. *Journal of Applied Business and Economics*, Vol. 16 No.1, pp. 84-9

Shropshire, J., Warkentin, M., Johnston, A. C., & Schmidt, M. B. (2006), "Personality and IT security: An application of the five-factor model", in *Proceedings of the Americas Conference on Information Systems AMCIS in Acapulco, México*, pp.3443-3449

Shropshire, J., Warkentin, M., and Sharma, S. (2015) Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49, pp. 177-191.

Spanos, G., Sioziou, A., and Angelis, L. (2013) WIVSS: A New Methodology for Scoring

Information Systems Vulnerabilities. In: *Proceedings of the 17th Panhellenic Conference on Informatics (PCI)*. 2013, ACM, pp. 83-90.

Statista - The Statistics Portal [Online]. Available at: http://statista.com.

Stewart, G. and Lacey, D. (2012) Death by a thousand facts: Criticizing the technocratic approach to information security awareness. *Information Management and Computer Security*, 20(1), pp. 29-38.

Sulaman, S., Weyns, K., and Host, M. (2013) A Review of Research on Risk Analysis Methods for IT Systems. In: *17th International Conference on Evaluation and Assessment in Software Engineering*. 2013, pp. 86-96.

Symantec, (2017) *Symantec Internet Security Threat Report*. Symantec Corporation.

Symantec, (2018) *Symantec Internet Security Threat Report*. Symantec Corporation

Takahashi, T., Emura, K., Kanaoka, A., Matsuo, S., and Minowa, T. (2013) Risk visualization and alerting system: Architecture and proof-of-concept implementation. In: *SESP'13*. 2013, ACM, pp. 3 -10.

Talib, S., Clarke, N., and Furnell, S. (2010) An Analysis of information security awareness within home and work environments. In: *International Conference on Availability, Reliability and Security*. 2010, IEEE, pp. 196 - 203.

Tamjidyamcholo, A., Yamchello, H., Bin, M., and Gholipour, R. (2013) Application of Fuzzy Set Theory to Evaluate The Rate of Aggregative Risk In Information Security. In: *International Conference on Research and Innovation in Information Systems (ICRIIS)*. 2013, pp. 410-415.

Tao, H., Liang, C., Chi, W., and Qun, H. (2010) The Research of Information Security Risk Assessment Method Based on Fault Tree. In: *6th International Conference on Networked Computing and Advanced Information Management (NCM)*. 2010, pp. 370-375.

The International Organization for Stanardization, The International Electrotechnical Commission (ISO/IEC), (2009) *ISO/IEC 31010:2009, Risk Management- Risk Assessment Techniques*. Switzerland.

The International Organization for Standardization, The International Electrotechnical Commission (ISO/IEC), (2011) *ISO/IEC 27005:2011, Information Technology- Security Techniques- Information Security Risk Management*. Switzerland.

Theoharidou, M., Mylonas, A., and Gritzalis, D. (2012) A Risk Assessment Method for Smartphones. *IFIP Advances in Information and Communication Technology*, 376, pp. 443-456.

Tiganoaia, B. (2012) Comparative Study Regarding The Tools Used for Security Risk Management. *Revista Academiei Fortelor Terestre*, 17(3), pp. 319-325.

Takahashi, K., Matsuzaki, T., Mine, T., Kawamura, T. and Sugahara K. (2011) Security as a Service for User Customized Data Protection. In: *International Conference on Software Engineering and Computer Systems (ICSECS 2011)*. 2011, Springer, pp. 298-309.

Tayouri, D. (2015) The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages. *Procedia Manufacturing*, Vol.3, pp. 1096-1100.

The Cambridge Analytica Files. Available from: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. [3 January 2019].

Uffen, J., Kaemmerer, N, and Breitner, M.H. (2013), "Personality Traits and Cognitive Determinants—An Empirical Investigation of the Use of Smartphone Security Measures", *Journal of Information Security*, Vol.4, pp. 203-212

Van Cleef, A. (2010) A Risk Management Process for Consumers: The Next Step in Information Security. In: *2010 Workshop on New security Paradigms (NSPW)*. 2010, pp. 107-114.

Vasileiou, I. and Furnell, S. (2018) Enhancing security education: Recognizing threshold concepts and other influencing factors. In: *(ICISSP) Proceedings of 4th International conference on information security and privacy,* Portugal, pp. 398-403.

Vermunt, J. and Verloop, N. (1999) Congruence and friction between learning and teaching. *Learning and Instruction*, 9(3), pp. 257-280.

Wahlberg, T., Paakkola, P., Wieser, C., Laakso, M., and Roning, J. (2013) Kepler - Raising browser security awareness. In: *Sixth International Conference on Software Testing, Verification and Validation Workshops*. 2013, IEEE, pp. 435 - 440.

Waltermire, D., Quinn, S., Scarfone, K.; Halbardier, A. (2011) The Technical Specification for The Security Content Automation Protocol (SCAP): SCAP Version 1.2. *NIST Special Publication 800-126 Revision 2.*

Warkentin, M., McBride, M., Johnston, A., and Carter, M. (2012) *The role of individual characteristics on insider abuse intentions*.

Wash, R. (2010) Folk models of home computer security. In: *Sixth Symposium on Usable Privacy and Security*. 2010, ACM, pp. 1 - 16.

Wash, R. and Rader, E. (2011) Influencing mental models of security: A research agenda. In: *NSPW' 11*. 2011, ACM, pp. 57 - 66.

Wangen. G. (2017) Information security risk assessment: A method comparison, *Computer ,* Vol.50, No.4, pp.52–61.

Wenge, O., Lampe, U. Rensing, C. and Steinmetz, R. (2014) Security information and event monitoring as a service: A survey on current concerns and solutions. *PIK-Praxis der Informationsverarbeitung und Kommunikation*, pp. 163-170.

Webb, J., Ahmad, A., Maynard, S., and Shanks, G. (2014) A situation awareness model for information security risk management. *Computers & Security*, 44, pp. 1-15.

WebWise (2015) [Online]. 2015. Available at: http://bbc.co.uk/webwise. (Accessed: 14 May 2015).

Willingham, D. (2009) *Why don't students like school?*. San Francisco, CA: Jossey-Bass.

Wilson, M. and Hash, J. (2003) Building and Information Technology Security Awareness and Training Program. *National Institute of Standards and Technology (NIST)*,

Workman, M. (2007) Wisecrackers: a theory grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society of Information Science and Technology*, Vol.59, pp. 662–674

Wright, J., McQueen, M., and Wellman, L. (2013) Analyses of two end-user software vulnerability exposure metrics (extended version). *Information Security Technical Report*, 17(4), pp. 173-184.

Wu, B. and Wang, A. (2011) EVMAT: An OVAL and NVD Based Enterprise Vulnerability Modeling and Assessment Tool. In: *Proceedings of the 49th Annual Southeast Regional Conference*. 2011, ACM, pp. 115-120.

Yazar, Z. (2011) A Qualitative Risk Analysis and Management Tool- CRAMM. *SANS Institue Information security Reading Room*,

Yalcin, Y., Kilic, B. (2018) Information Security Risk Management and Risk Assessment Methodology and Tools. *In (ICONCS'18) International Conference on Cyber Security and Computer Science*, 2018, pp.73-78.

Yousif, M (2016) Biometrics-as-a-Service – The Final Frontier of Security. *Cloud Computing*, Vol.5, No.4, pp.4-5.

Yu, L., Motopalli, S., Lee, D., Liu, P., Xu, H., Liu, Q., Tan, J. and Luo, B. (2018) My Friend Leaks My Privacy: Modeling and Analyzing Privacy in Social Networks. In: *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies (SACMAT '18)*, 2018, ACM, pp.93-104.

Zabaa, Z., Furnell, S., and Dowland, P. (2011) End- user Perception and Usability of Information Security. In: *5th International Symposium on Human Aspects of Information Security and Assurance (HAISA)*. 2011, pp. 97-107.

Zambon, E., Etalle, S., Wieringa, R., and Hartel, P. (2010) Model-based qualitative risk assessment for availability of IT infrastructures. *Softw Syst Model*, 10(4), pp. 553-580.

Zhang, L. (2006) Thinking styles and the big five personality traits revisited. *Personality and Individual Differences,* Vol.40 No.6, pp.1177-1187.

Publications

I. Journal publications:

1) Alohali, M., Clarke, N., Li, F. and Furnell, S. (2018). Identifying and Predicting the Factors Affecting End-users' Risk-taking Behavior. *Information and Computer Security*, Vol.26, Issue 3, pp.306-326.
DOI: 10.1108/ICS-03-2018-0037
ISSN: 2056-4961.

2) Alohali, M., Clarke, N. and Furnell, S. (2018). The Design and Evaluation of a User-centric Information Security Risk Assessment and Response Framework. *International Journal of Advanced Computer Science and Applications, ,* Vol.9, Issue 10, pp.148-163.
DOI: 10.14569/IJACSA.2018.091018
ISSN: 2156-5570.

II. Conference publications:

1) Alohali, M., Clarke, M., Furnell, S. and Albakri, S. (2017). Information Security Behavior: Recognizing the Influencers. *Computing Conference*, London, United Kingdom, 2017, pp. 844-853.
DOI: 10.1109/SAI.2017.8252194
ISBN: 978-1-5090-5443-5.

2) Alohali, M., Clarke, N., Li, F. and Furnell, S. (2017). Identifying the Factors Affecting End-Users' Risk-Taking Behavior. *Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017)*, Adelaide, Australia, 2017, pp. 126-144.
ISBN: 978-1-84102-428-8